

CommandCenter® Secure Gateway



CC-SG Administrator Guide Release 3.0

Copyright © 2006 Raritan, Inc.

CCA-0B-E

May 2006

255-80-5140-00

This page intentionally left blank.

Copyright and Trademark Information

This document contains proprietary information that is protected by copyright. All rights reserved. No part of this document may be photocopied, reproduced, or translated into another language without express prior written consent of Raritan, Inc.

© Copyright 2006 Raritan, CommandCenter, RaritanConsole, Dominion, and the Raritan company logo are trademarks or registered trademarks of Raritan, Inc. All rights reserved. Java is a registered trademark of Sun Microsystems, Inc. Internet Explorer is a registered trademark of Microsoft Corporation. Netscape and Netscape Navigator are registered trademarks of Netscape Communication Corporation. All other marks are the property of their respective owners.

FCC Information

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a commercial installation. This equipment generates, uses, and can radiate radio frequency energy and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. Operation of this equipment in a residential environment may cause harmful interference.

Japanese Approvals

この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

Raritan is not responsible for damage to this product resulting from accident, disaster, misuse, abuse, non-Raritan modification of the product, or other events outside of Raritan's reasonable control or not arising under normal operating conditions.



*For assistance in the North or South America, please contact the Raritan Technical Support Team by telephone (732) 764-8886, by fax (732) 764-8887, or by e-mail tech@raritan.com
Ask for Technical Support – Monday through Friday, 8:00am to 8:00pm, Eastern.*

For assistance around the world, please see the last page of this guide for regional Raritan office contact information.

Safety Guidelines

To avoid potentially fatal shock hazard and possible damage to Raritan equipment:

- Do not use a 2-wire power cord in any product configuration.
- Test AC outlets at your computer and monitor for proper polarity and grounding.
- Use only with grounded outlets at both the computer and monitor. When using a backup UPS, power the computer, monitor and appliance off the supply.

Rack Mount Safety Guidelines

In Raritan products which require Rack Mounting, please follow these precautions:

- Operation temperature in a closed rack environment may be greater than room temperature. Do not exceed the rated maximum ambient temperature of the appliances (see **Appendix A: Specifications**).
- Ensure sufficient airflow through the rack environment.
- Mount equipment in the rack carefully to avoid uneven mechanical loading.
- Connect equipment to the supply circuit carefully to avoid overloading circuits.
- Ground all equipment properly, especially supply connections, such as power strips (other than direct connections), to the branch circuit.

Contents

Chapter 1: Introduction	1
Prerequisites	1
Intended Audience	1
Product Photos.....	1
Product Features and Benefits	2
Terminology/Acronyms	3
New 3.0 Features.....	6
Chapter 2: Accessing CC-SG.....	7
Browser-Based Access	7
Standalone Client Access	9
Confirm IP Address.....	9
Check and Upgrade CC-SG Firmware Version	10
Check and Upgrade Application Versions	10
Connection to Console and KVM Management Appliances	11
Power Down CC-SG	13
CC-SG Window Components	13
Overview	14
Main Window Components.....	15
Configuring CC-SG Manager Components	16
Configurable Parameters.....	16
Compatibility Matrix.....	17
Chapter 3: Example Configuration Workflow	19
Create Associations	19
Add Devices	22
Configure Ports	24
Serial Port.....	24
KVM Port.....	26
Add Users to System Administrators Group	27
Control User Access	28
Create User Groups.....	28
Create/Edit Port Groups	30
Create/Edit Policies	31
Apply Policies to User Groups	32
Add Users to User Group	33
Chapter 4: Creating Associations.....	35
Associations	35
Associations-Defining Categories and Elements	35
Association Terminology.....	36
How to Create Associations.....	37
Association Manager.....	37
Add Category.....	38
Edit Category	39
Delete Category.....	39
Add Element	40
Edit Element	41
Delete Element	41
Association Wizard.....	42
Import Categories, Devices, Ports from CSV File.....	45
CSV File Format	46
CSV File Example.....	46
Chapter 5: Adding Devices and Device Groups.....	49
Device Manager	49
Device Icons	50
Add Device	51
Edit Device	54
Delete Device	55
Bulk Copy	55
Backup Device Configuration	56
Restore Device Configuration.....	56

Copy Device Configuration	57
Upgrade Device	57
Ping Device	58
Restart Device	58
Pause Device	59
Resume Device	59
View Devices.....	59
Regular View	59
Custom View	60
Add Custom View	61
Edit Custom View	61
Delete Custom View	62
Topological View.....	63
Special Access to Paragon II System Devices	64
Paragon II System Controller (P2-SC).....	64
IP-Reach and UST-IP Administration	65
Device Power Manager.....	66
Discover Devices	67
Device Group Manager	69
Add Device Group	69
Edit Device Group Name	70
Delete Device Group	71
Add Device Rule	71
Delete Device Rule	72
Search for Devices.....	73
Navigation Tips.....	73
Supported Wildcards	73
Disconnect Users	74
Chapter 6: Configuring Ports and Port Groups	75
Port Manager	75
Port Icons	77
Configure Port	78
Edit Port.....	88
Port Group Manager	91
Chapter 7: Adding Users and User Groups	93
Add User	93
Edit User	94
Change User Password.....	95
Change Own Password	95
Delete User	96
Logoff User(s)	97
Bulk Copy.....	98
Add User to Group	99
Delete User from Group.....	99
Default User Groups	99
Add User Group	100
Edit User Group	101
Apply (Edit) User Group Policies	102
Delete User Group	103
Assign Users to Group.....	103
Search for Users	104
Navigation Tips.....	104
Supported Wildcards	105
Chapter 8: Creating Policies.....	107
Controlling User Access with Policies.....	107
Policy Terminology	107
User Groups	108
Port Groups	108
Device Groups.....	108
Policies	109
Apply Policies to User Group.....	109
Policy Summary.....	109
Policy Manager	110
Add Policy.....	110

Edit Policy	111
Delete Policy	112
Chapter 9: Configuring Remote Authentication	113
Authentication and Authorization	113
Flow for Authentication	113
User Accounts	113
Establish Order of Authentication Databases	114
Distinguished Names for LDAP and Active Directory	114
Username	114
Base DN	115
Active Directory (AD)	115
Setup on AD Server	115
Setup on CC-SG	117
General Settings on CC-SG	118
Advanced Settings on CC-SG	119
Group Settings on CC-SG	121
LDAP (Netscape)	124
Sun One LDAP (iPlanet) Configuration Settings	127
OpenLDAP (eDirectory) Configuration Settings	127
TACACS+	128
RADIUS	130
Certificate	131
Export Current Certificate and Private Key	131
Generate Certificate Signing Request	132
Generate Self Signed Certificate Request	133
IP-ACL	134
Chapter 10: Generating Reports	135
Active Users Report	135
Active Ports Report	136
Asset Management Report	137
Audit Trail Report	138
Error Log Report	140
Ping Report	142
Accessed Devices Report	143
Group Data Report	145
User Data Report	146
Users In Groups Report	147
Query Port Report	148
View Stored Reports	149
Locked Out Users Report	150
CC-NOC Synchronization Report	151
Chapter 11: System Maintenance	153
Reset CC-SG	153
Backup CC-SG	153
Restore CC-SG	154
Saving and Uploading Backup Files	155
Refresh CC-SG Display	156
Upgrade CC-SG	157
Restart CC-SG	157
Shut Down CC-SG	158
Restart CC-SG after Shutdown	158
End CC-SG Session	159
Log Out	159
Exit CC-SG	159
Maintenance Mode	159
Scheduled Tasks	160
Entering Maintenance Mode	160
Exiting Maintenance Mode	160
Chapter 12: Advanced Administration	161
Configuration Manager	161
Network Configuration	161
Log Configuration	163

Inactivity Timer Configuration	164
Time/Date Configuration	165
Modem Configuration	166
Connection Mode	172
Device Settings	174
SNMP	175
Configure Security	176
Strong Password Rules	177
Enable User Lockout	177
Application Manager	178
Add Application	178
Edit Application	179
Delete Application	180
Firmware Manager	180
Upload Firmware	180
Delete Firmware	181
CommandCenter NOC	181
Add a CC-NOC	182
Edit a CC-NOC	185
Launch CC-NOC	186
Delete a CC-NOC	187
Cluster Configuration	187
Create a Cluster	188
Remove Secondary CC-SG Node	190
Remove Primary CC-SG Node	190
Recover a Failed CC-SG Node	190
Set Advanced Settings	191
Task Manager	191
Task Types	191
Scheduling Sequential Tasks	192
Email Notifications	192
Stored Reports	192
Create a New Task	193
View a Task, Details of a Task, and Task History	195
Notification Manager	197
SSH Access to CC-SG	198
Command Tips	200
Create a SSH Connection to an SX Device	201
Connect to a Serial Port	202
Exit a Session	203
Diagnostic Console	204
Accessing Diagnostic Console via SSH	204
Accessing Status Console	205
Accessing Administrator Console	206
Appendix A: Specifications (G1, V1)	225
G1 Platform	225
General Specifications	225
Hardware Specifications	225
Remote Connection	225
Environmental Requirements	225
Electrical Specifications	226
V1 Platform	227
General Specifications	227
Hardware Specifications	227
Remote Connection	227
Environmental Requirements	227
Electrical Specifications	228
Appendix B: CC-SG and Network Configuration	229
Introduction	229
Executive Summary	229
CC-SG Communication Channels	231
CC-SG and Raritan Devices	231
CC-SG Clustering	231
Access to Infrastructure Services	232
PC Clients to CC-SG	232
PC Clients to Targets	233
CC-SG & Client for IPMI, iLO/RILOE, Etc.	233

CC-SG & SNMP	234
CC-SG & CC-NOC	234
CC-SG Internal Ports.....	234
CC-SG Access via NAT-enabled Firewall.....	234
Security and Open Port Scans.....	235
Appendix C: Initial Setup Process Overview	237
Appendix D: User Group Privileges.....	239
Appendix E: SNMP Traps	243
Appendix F: Troubleshooting.....	245
Client Browser Requirements	245
Import CSV File (Category, Device, Port) Error Message	245
Port and Policy Group Creation Failure	246
Appendix G: FAQs	247

Figures

Figure 1 CC-SG Front View	1
Figure 2 CC-SG - Rear Panel	1
Figure 3 Security Alert Window.....	7
Figure 4 Login Window	8
Figure 5 CC-SG Application Window	8
Figure 6 IP Specification Window	9
Figure 7 Set IP Address with Configuration Manager Commands	9
Figure 8 Upgrade CC-SG.....	10
Figure 9 CC-SG Application Manager	10
Figure 10 CC-SG Application Search Window.....	11
Figure 11 Security Warning for Signed Console Applet	12
Figure 12 RaritanConsole Application.....	12
Figure 13 CC-SG Application Window	15
Figure 14 Compatibility Matrix.....	17
Figure 15 Association Wizard Overview	19
Figure 16 Association Wizard - Category and Elements Screen.....	20
Figure 17 Adding Another Category.....	21
Figure 18 Association Wizard - Confirm Choices.....	21
Figure 19 Association Wizard - Summary Screen.....	22
Figure 20 Add Device CC-SG	22
Figure 21 Add Device PowerStrip	23
Figure 22 Add Device SX.....	23
Figure 23 Configuration Ports	24
Figure 24 Configure Serial Ports.....	25
Figure 25 Configure Ports	26
Figure 26 Configure KVM Port	26
Figure 27 Add User Screen.....	27
Figure 28 Add User Group Screen.....	29
Figure 29 Port Groups Manager Screen	30
Figure 30 Add Port Group Window	30
Figure 31 Policy Manager Screen	31
Figure 32 Update Policy Window	32
Figure 33 Edit User Group Policies Screen.....	32
Figure 34 Add User Screen.....	33
Figure 35 CC-SG Organization Example	35
Figure 36 Association Manager Screen	38
Figure 37 Add Category Window	38
Figure 38 Edit Category Window	39
Figure 39 Delete Category Window	39
Figure 40 Association Manager Screen	40
Figure 41 Add Element Window.....	40
Figure 42 Edit Element Window.....	41
Figure 43 Delete Element Window.....	41
Figure 44 Association Wizard Overview	42
Figure 45 Association Wizard - Category And Elements Screen	42
Figure 46 Adding Another Category.....	43
Figure 47 Association Wizard - Confirm Choices.....	43
Figure 48 Association Wizard - Summary Screen.....	44
Figure 49 Import Categories Screen	45
Figure 50 Analysis Report Screen	47
Figure 51 The Devices Tab And View Devices Screen.....	49

Figure 52 Add Device Selection Screen	51
Figure 53 Add Device Screen for PowerStrip.....	51
Figure 54 Add Device Screen for Raritan Devices.....	52
Figure 55 Add Device Screen for iLO, RILOE.....	52
Figure 56 Add Device Screen for IPMI Server (v 1.5)	53
Figure 57 Add Device Screen for Generic Device.....	53
Figure 58 Edit Device Screen	54
Figure 59 Delete Device Screen	55
Figure 60 Bulk Copy Screen	55
Figure 61 Backup Device Configuration Screen	56
Figure 62 Restore Device Configuration Screen.....	56
Figure 63 Copy Device Configuration Screen	57
Figure 64 Upgrade Device Screen.....	57
Figure 65 Ping Device Screen	58
Figure 66 Restart Device Screen	58
Figure 67 Devices Tree Regular View Screen	59
Figure 68 Custom View Screen	60
Figure 69 Add Custom View Window.....	61
Figure 70 Edit Custom View Window.....	61
Figure 71 Custom View Screen	62
Figure 72 Delete Custom View Window.....	62
Figure 73 Topological View Screen	63
Figure 74 Paragon System Launch Admin Menu Option	64
Figure 75 Paragon Manager Application Window	64
Figure 76 Remote User Station Admin Option	65
Figure 77 IP-Reach Administration Screen	65
Figure 78 Device Power Manager Screen	66
Figure 79 Discover Devices Screen.....	67
Figure 80 Discovered Devices List Window.....	67
Figure 81 Add Device Screen	68
Figure 82 Device Groups Manager Screen.....	69
Figure 83 Add Device Group Window	69
Figure 84 Device Groups Manager Screen.....	70
Figure 85 Edit Device Group Window	70
Figure 86 Device Groups Manager Screen.....	71
Figure 87 Delete Device Group Window.....	71
Figure 88 Device Groups Manager Screen.....	71
Figure 89 Device Groups Manager Screen.....	72
Figure 90 Delete Rule Window	72
Figure 91 Search for Devices.....	73
Figure 92 Disconnect Users.....	74
Figure 93 The Ports Tab And View KVM Port Screen	76
Figure 94 Configure Ports Screen.....	78
Figure 95 Configure Serial Ports Screen	79
Figure 96 Associated Generic Device with a Serial Port.....	79
Figure 97 In-Band Parameters.....	80
Figure 98 Configure Ports Screen.....	81
Figure 99 Configure KVM Port Screen.....	81
Figure 100 In-Band Parameters.....	82
Figure 101 Associated Generic Device with a KVM Port	82
Figure 102 Configure Ports Screen.....	83
Figure 103 Configure Generic Ports Screen	83
Figure 104 Configure Ports Screen for Powerstrip Device.....	84

Figure 105 Configure Ports Screen for IPMI Server.....	84
Figure 106 Configure Outlet Port Screen.....	85
Figure 107 Delete Port Screen.....	86
Figure 108 Bulk Copy Screen.....	87
Figure 109 Edit Serial Port Screen.....	88
Figure 110 Edit KVM Port Screen.....	89
Figure 111 Edit Generic Port Screen.....	90
Figure 112 Port Groups Manager Screen.....	91
Figure 113 Add Port Group Window.....	91
Figure 114 Edit Port Group Window.....	92
Figure 115 Delete Port Group Window.....	92
Figure 116 Add User Screen.....	93
Figure 117 Edit User Screen.....	94
Figure 118 Change User Password Screen.....	95
Figure 119 Change My Profile Screen.....	95
Figure 120 Delete User Screen.....	96
Figure 121 Logoff Users Screen.....	97
Figure 122 Bulk Copy Screen.....	98
Figure 123 Add User To Group Screen.....	99
Figure 124 Delete User From Group Screen.....	99
Figure 125 Add User Group Screen.....	100
Figure 126 Edit User Group Screen.....	101
Figure 127 Edit User Group Policies Screen.....	102
Figure 128 Group Delete User Group Screen.....	103
Figure 129 Assign Users in Group Screen.....	103
Figure 130 Search for Users.....	104
Figure 131 Ports, Port Groups, Policies, User Groups, Users.....	109
Figure 132 Policy Manager Screen.....	110
Figure 133 Add Appliance Policy Window.....	110
Figure 134 Update Policy Window.....	111
Figure 135 Edit Appliance Policy Window.....	111
Figure 136 Update Policy Window.....	111
Figure 137 Delete Appliance Policy Window.....	112
Figure 138 Security Manager General Screen.....	114
Figure 139 Active Directory Account.....	115
Figure 140 Active Directory Users.....	116
Figure 141 Assigning User to a Group.....	116
Figure 142 Specifying a Name for Active Directory Server.....	117
Figure 143 Specifying General Values for Active Directory Server.....	118
Figure 144 Specifying Advanced Values for Active Directory Server.....	119
Figure 145 Specifying Group Values for Active Directory Server.....	121
Figure 146 Importing Groups from Active Directory Server.....	122
Figure 147 Viewing Privileges of Imported Group.....	122
Figure 148 Viewing Policy of Imported Group.....	123
Figure 149 Logging In as Remotely Authenticated User.....	123
Figure 150 Security Manager Add Module Screen.....	124
Figure 151 Security Manager LDAP Screen General Tab.....	125
Figure 152 Security Manager LDAP Screen Advanced Tab.....	126
Figure 153 Security Manager Add Module Screen.....	128
Figure 154 Specifying a TACACS+ Server.....	129
Figure 155 Security Manager Add Module Screen.....	130
Figure 156 Specifying a RADIUS Server.....	130
Figure 157 Security Manager Certificate Screen.....	131

Figure 158 Generate Certificate Signing Request Screen	132
Figure 159 Certificate Request Generated.....	132
Figure 160 Generate Self Signed Certificate Window	133
Figure 161 Security Manager IP-ACL Screen	134
Figure 162 Active Users Report	135
Figure 163 Manage Report Window	136
Figure 164 Active Ports Report	136
Figure 165 Asset Management Report	137
Figure 166 Audit Trail Screen	138
Figure 167 Audit Trail Report	139
Figure 168 Error Log Screen.....	140
Figure 169 Error Log Report	141
Figure 170 Ping Report.....	142
Figure 171 Accessed Devices Screen	143
Figure 172 Accessed Devices Report	144
Figure 173 Groups Report	145
Figure 174 All Users' Data Report	146
Figure 175 Users In Groups Report	147
Figure 176 Query Port Report.....	148
Figure 177 View Stored Reports	149
Figure 178 Locked Out Users Report	150
Figure 179 CC-NOC Synchronization Report	151
Figure 180 Reset CC-SG Screen.....	153
Figure 181 Backup CC-SG Screen	153
Figure 182 Restore CC-SG Screen	154
Figure 183 Browse to Upload a Backup of CC-SG	155
Figure 184 Refresh Shortcut Button.....	156
Figure 185 Upgrade CC-SG Screen	157
Figure 186 Restart Screen.....	157
Figure 187 Info Window	158
Figure 188 Shutdown CC-SG Screen	158
Figure 189 Logout Window	159
Figure 190 Exit Window	159
Figure 191 Enter Maintenance Mode.....	160
Figure 192 Configuration Manager Network Settings Screen	161
Figure 193 Primary/Backup Network	162
Figure 194 Active/Active Network	162
Figure 195 Configuration Manager Logs Screen	163
Figure 196 Configuration Manager Inactivity Timer Screen	164
Figure 197 Configuration Manager Time/Date Screen.....	165
Figure 198 Configuration Manager Modem Screen	166
Figure 199 Modems Tab.....	166
Figure 200 Extra Initialization Commands.....	167
Figure 201 Create a new connection	167
Figure 202 New Connection Wizard	168
Figure 203 Connection Name	168
Figure 204 Phone Number to Dial.....	168
Figure 205 Specify Dial-up Script.....	169
Figure 206 Connecting to CC-SG	170
Figure 207 Entering username and password	170
Figure 208 After Dial Terminal	171
Figure 209 Configuration Manager Connection Screen – Direct Mode or Proxy Mode.....	172
Figure 210 Configuration Manager Connection Screen – Both.....	173

Figure 211 Configuration Settings Device Settings Screen.....	174
Figure 212 Configuration Settings Device Settings Screen.....	175
Figure 213 Security Manager General Screen.....	176
Figure 214 Lockout Settings	177
Figure 215 Error (User Being Locked Out) Screen	178
Figure 216 Application Manager Screen.....	178
Figure 217 Add Application Window	178
Figure 218 Search Window.....	179
Figure 219 Edit Application Window	179
Figure 220 Delete Application Window	180
Figure 221 Firmware Manager Screen	180
Figure 222 Search Window.....	181
Figure 223 Delete Firmware Window.....	181
Figure 224 CC-NOC Configuration Screen.....	182
Figure 225 CC-NOC Configuration Screen.....	182
Figure 226 Add CC-NOC Configuration Screen.....	183
Figure 227 CC-NOC Passcodes	184
Figure 228 CC-NOC Configuration Screen	185
Figure 229 Edit CC-NOC Configuration Screen.....	186
Figure 230 Launch CC-NOC.....	186
Figure 231 Delete CC-NOC Screen.....	187
Figure 232 Cluster Configuration Screen.....	188
Figure 233 Cluster Configuration – Primary Node Set.....	188
Figure 234 Cluster Configuration – Set Secondary CC-SG	189
Figure 235 Recovering a node from Waiting status	190
Figure 236 Cluster Configuration Advanced Settings	191
Figure 237 Task Manager	193
Figure 238 Create Task	193
Figure 239 Selecting a Task to Schedule.....	194
Figure 240 Specifying Task Recurrence	194
Figure 241 Specifying Task Email Notification	195
Figure 242 View a Task	195
Figure 243 Task History	196
Figure 244 Task Details	196
Figure 245 Notification Manager	197
Figure 246 SSH Client	198
Figure 247 Login to CC-SG via SSH.....	198
Figure 248 CC-SG Commands via SSH	199
Figure 249 SSH Help	199
Figure 250 SSH listfirmwares Help	200
Figure 251 Listing Devices on CC-SG	201
Figure 252 Access SX Device via SSH.....	201
Figure 253 Listing Ports on CC-SG.....	202
Figure 254 Connecting to a Serial Port.....	202
Figure 255 SSH Client	204
Figure 256 Login to Status Console.....	205
Figure 257 Status Console.....	205
Figure 258 Login to Administrator Console	206
Figure 259 Administrator Console.....	206
Figure 260 Selecting to Edit Pre-Login Message	207
Figure 261 Editing MOTD for Status Console	207
Figure 262 Selecting to Edit Status Console Config	208
Figure 263 Edit Status Console Config	209

Figure 264 Selecting Network Interface Configuration	209
Figure 265 Editing Network Interfaces	210
Figure 266 Pinging a Target.....	211
Figure 267 Performing Traceroute on a Target.....	212
Figure 268 Selecting Static Routes	213
Figure 269 Editing Static Routes.....	213
Figure 270 Viewing Log Files.....	213
Figure 271 Selecting Log Files to View	214
Figure 272 Selecting Log Files to View.....	215
Figure 273 Changing Colors in Log Files	215
Figure 274 Displaying Information	215
Figure 275 Adding Expressions in Log Files	216
Figure 276 Specifying a Regular Expression for a Log File	216
Figure 277 Getting Help (F1)	217
Figure 278 Selecting CC-SG Restart in Diagnostic Console.....	217
Figure 279 Restarting CC-SG in Diagnostic Console	218
Figure 280 Selecting CC-SG System Reboot in Diagnostic Console.....	218
Figure 281 Rebooting CC-SG in Diagnostic Console	219
Figure 282 Password Configuration.....	219
Figure 283 Configuring Password Settings	220
Figure 284 Account Configuration.....	221
Figure 285 Configuring Accounts	221
Figure 286 Selecting Disk Status in Diagnostic Console	222
Figure 287 Displaying Disk Status of CC-SG in Diagnostic Console	223
Figure 288 Selecting Top Display in Diagnostic Console.....	223
Figure 289 Displaying CC-SG Processes in Diagnostic Console.....	224
Figure 290 Association Management Process.....	237
Figure 291 Port Group Failure	246

Chapter 1: Introduction

Congratulations on your purchase of CommandCenter Secure Gateway (CC-SG), Raritan's convenient and secure method for managing various UNIX servers, firewalls, routers, load balancers, Power Management devices, and Windows servers.

CC-SG provides central management and administration, using a set of serial and KVM appliances. It is designed to operate in a variety of environments, from high-density Data Centers to Service Provider environments to corporate environments handling large remote offices.

CC-SG, when used in conjunction with Raritan's Dominion or IP-Reach port-level management appliances, streamlines and simplifies the management of the target devices, easing administration of data center equipment by connecting to the IP network and presenting the serial console and KVM ports of all the target devices within the managed network.

Prerequisites

Before configuring a CC-SG according to the procedures in this document, refer to Raritan's **CommandCenter Secure Gateway Setup Guide** for instructions on how to quickly install CC-SG and its managed devices. Refer to Raritan's **Digital Solution Deployment Guide** for more comprehensive instructions on deploying Raritan devices that are managed by CC-SG.

Intended Audience

This document is intended for Administrators who reside in the System Administrator user group. These administrators typically have all privileges—please see **Appendix D: User Group Privileges**. Users that reside outside these groups usually have fewer privileges, such as being granted only the Ports Access privilege—please refer to Raritan's **CommandCenter Secure Gateway User Guide** for additional information.

Product Photos



Figure 1 CC-SG Front View



Figure 2 CC-SG - Rear Panel

Product Features and Benefits

- **Seamless Management**

CC-SG offers seamless management of Dominion series and Paragon® management appliances through Paragon remote User Stations (UST1R/UST2R) – leverage your embedded base with a CC-SG to draw substantial incremental value:

- Constantly updated to keep up with changing needs.
- Streamlines, provides wider process focus and offers productivity improvements, organization wide.
- Reduces Total Cost of Ownership (TCO); cost savings from high-availability of applications (high cost for downtime); front-ends and secures and improves reliability of high economic value equipment.
- Handles scalability elegantly – multiple data centers (primary and backup), growing number of locations.
- Provides centralized management, Role-Based Access and Control (RBAC), and Reporting Capabilities.

- **Uncompromising Security**

Secure 128-bit encryption (both intranet and Internet); flexibility of access via SSL, access restriction (by time of day, and/or maximum session duration) as part of user profile in user management:

- Has the ability to restrict login access to products based on time of day, the ability to restrict duration of on-line sessions, handle password expiration, and prompt for password changes. All user operations, including access to port history buffer and access to logs, will be granted or denied based on user authorization level.
- IP ACL (IP-Filtering) – grants/restricts access by domain name or IP addresses.
- Grants or restricts access on an individual user basis.
- Supports primary and secondary servers.
- Fallback authentication through local database

- **Single IP Address Access**

Reduces the complexities of managing multiple IP addresses with associated user names and passwords.

- **Broad Support for Third Party Authentication**

Leverages existing investment in authentication protocols and allows centralized authentication and authorization. Streamlines deployment of large multi-unit systems and centralizes administration and control. Supports LDAP (including AD, iPlanet, eDirectory), RADIUS, and TACACS+. Support for Active Directory® authorization and the importing of user groups.

- **Comprehensive Administration Tools**

Reduces TCO for managing IT infrastructure; found time can be used for proactive maintenance:

- Provides powerful multi-tiered user and permissions grouping (user/leaf nodes, targets by topology and by function); CC-SG's powerful, user-customizable categorization allows you to easily tailor your solution and security, for example, create a "Location" attribute and assign all users in a given LDAP or Active Directory group access to servers in that Location). The possibilities are limitless!
- Provides powerful user-customizable views of all devices connected to CC-SG; supports automatic and manual device discovery.
- Simplifies administration – device upgrade, reset, diagnosis, ping, auto discover, edit, delete firmware upgrades, monitoring and access for back up, retrieval and push-down of configuration to leaf nodes (Dominion Series); simplifies daily maintenance and firmware management.

- **Flexible Reporting**

Provides adjustable ways to view active devices, users, ports, and asset inventory; reports include Audit Trail, Error Log, Firmware Report, Ping Report, View By Groups, and Users in Groups.

- **Comprehensive Logging**
 - Logs events locally.
 - Can use an external syslog server for event logs (events are immediately posted or exported) and the ability to have other Raritan products use it as a syslog server.
 - Provides full auditing and tracking capabilities.
 - Keeps an audit trail for tracking user activity.
- **Support for SNMP Agents and Traps**
 - Provides SNMP GET/SET operations with third-party enterprise Management Solutions, such as HP OpenView. To support the operations, you must provide SNMP agent identifier information such as these MIB-II System Group objects: sysContact, sysName, and sysLocation.
 - Provides System level trap notification of CC-SG's operational events.
 - Provides Application level trap notification regarding the monitoring of managed devices, availability events, and the audit events of user access and authorization to CC-SG.
- **Infrastructure Support for Customizable Applets via GUI**
 - Customizable applets control ranges of devices including power strips, HP's iLO/RILOE cards, etc.
 - Target systems accessed through applets – remote access to servers and other data center equipment managed by Raritan management appliances through downloadable applets/COM controls.
 - Power strip outlet user authorization setting, mapping, parameter-passing, target server-mapping.
- **Access to CommandCenter NOC® (CC-NOC)**
For detailed auditing, monitoring and notification of infrastructure and Raritan devices.
- **Operational Flexibility/Ease of Use/Administrator Presentation**
Enhanced system setup entirely through graphical user interface (state-of-the-art UI standards with professional look and feel).
- **Designed for High Availability**
 - ATA Raid-1 card and two ATA hard drivers to provision for fault-tolerance at the hardware and OS level.
 - Two network interfaces for failover or to be configured for public and private IP addresses on separate NICs.
 - Redundant power supplies and ECC memory.
 - Auto-recovery (watchdog timer).
 - Modem access for emergency administration.
 - Support for primary and secondary servers.
- **Support for Clustering and Geographic Redundancy**
Enabling backup availability with CC-SGs located on the same or different networks.
- **Internationalization**
Language, keyboard, scope of support; documentation available in French, German, Japanese, Traditional Chinese, Simplified Chinese, and Korean.

Terminology/Acronyms

Terms and acronyms found in this document include:

- **Associations**—is the relationship between categories, elements of a category, and ports or devices or both. For example, if you want to associate the “Location” category with a device, Create associations first before adding devices and ports in CC-SG.
- **Category**—is a variable that contains a set values or elements. An example of a Category is Location, which may have elements such as “New York City”, “Philadelphia”, or “Data Center 1”. When you add devices and ports to CC-SG, you will associate this information with them. It is easier if you set up associations correctly first, before adding devices and ports to them. Another example of a Category is “OS Type”, which may have elements such as “Windows®” or “Unix®” or “Linux®”.

- **CIM** (Computer Interface Module)—is the hardware used to connect a target server and a Raritan device. Each target requires a CIM, except for the Dominion KX101 which is attached directly to one target and therefore, does not require a CIM. Targets servers should be powered on and connected to CIMs and CIMs should be connected to the Raritan Device BEFORE adding the ports in CC-SG. Otherwise, the blank CIM name will overwrite the CC-SG port name. Servers need to be rebooted after connecting to a CIM.
- **CommandCenter NOC (CC-NOC)**—is a network monitoring appliance that audits and monitors the status of servers, equipment, and Raritan devices that CC-SG manages.
- **Device Group**—a defined group of devices (see the **Devices** definition) that are accessible to a user. Device groups are used when creating a policy to control access to the devices in the group.
- **Devices**—are Raritan products such as Dominion KX116, Dominion SX48, Dominion KSX440, IP-Reach, Paragon II System Controller, Paragon II UMT832 with USTIP, etc. that are managed by CC-SG. These devices control the target servers and systems that are connected to them.
- **Elements**—are the values of a category. For example, the “New York City” element belongs to the “Location” category. Or, the “Windows” element belongs to the “OS Type” category.
- **Generic Devices**—a device, such as a hub, Windows server, or Cisco router, that can be managed by CC-SG. Generic devices cannot be discovered by CC-SG; they have to be manually added—see section **Add Device** in **Chapter 5: Adding Devices and Device Groups**.
- **Ghosted Ports**—a ghosted port can occur when managing Paragon devices and when a CIM or target server is removed from the system or powered off (manually or accidentally). Refer to Raritan’s *Paragon II User Manual* for additional information.
- **Hostname**—A hostname can be used if DNS server support is enabled (see section **Network Configuration** in **Chapter 12: Advanced Administration** for additional information). The hostname and its Fully-Qualified Domain Name (FQDN = Hostname + Suffix) cannot exceed 257 characters. It can consist of any number of components, as long as they are separated by “.”. Each component has a maximum size of 63 characters and the first character must be alphabetic. The remaining characters can be alphabetic, numeric, or “-“ (hyphen or minus). The last character of a component may not be “-”. While the system preserves the case of the characters entered into the system, the FQDN is case-insensitive when used.
- **iLO/RILOE**—Hewlett Packard’s Integrated Lights Out/Remote Insight Lights Out servers that can be managed by CC-SG. Data between CC-SG and iLO/RILOE device is SSL encrypted. Targets of an iLO/RILOE device are powered on/off and recycled directly. iLO/RILOE devices cannot be discovered by CC-SG; they have to be manually added—see section **Add Device** in **Chapter 5: Adding Devices and Device Groups**.
- **In-band Access**—going through the TCP/IP network to correct or troubleshoot a target in your network. KVM, Serial, and Generic devices can be accessed via these in-band applications: **RemoteDesktop Viewer**, **SSH Client**, **VNC Viewer**.
- **IPMI Servers** (Intelligent Platform Management Interface)—servers that can be controlled by CC-SG. IPMI are discovered automatically but can be added manually as well—see section **Add Device** in **Chapter 5: Adding Devices and Device Groups**.
- **Out-of-Band Access**—using applications such as Raritan Remote Console (RRC), Raritan Console (RC), or Multi-Platform Client (MPC) to correct or troubleshoot a KVM or serial managed target in your network.
- **Policies**—define the permissions, type of access, and to which ports and/or devices a user group has access to. Policies are applied to a user group and have several control parameters to determine the level of control, such as date and time of access.
- **Port Groups**—a defined group of ports that are accessible to a user. Port groups are used when creating a policy to control access to the ports in the group.

- **Ports**—are connection points between a Raritan Device and a target system or server. Or, a port can be a device that is directly connected to a LAN/CC-SG via In-band access. In CC-SG, you click on a port to access and manage the target. The port is essentially the destination system and should be named appropriately for that system, for example, **NYC_SunSRV1**.
- **SASL**—(Simple Authentication and Security Layer). A method for adding authentication support to connection-based protocols.
- **SSH**—clients, such as Putty or OpenSSH, provide a command line interface to CC-SG. Only a subset of CC-SG commands is provided via SSH to administer devices and CC-SG itself—please see **Chapter 12: Advanced Administration** for additional information.
- **Target Usernames**—specified when configuring in-band parameters of a serial, KVM, or generic port. When a name is specified, only a password is required when accessing the target.
- **User Groups**—are a set of users that share the same level of access and privileges. For example, the default user group **System Administrators** has full access to all configuration tasks and target hosts and servers. All other user groups have restricted CC-SG access and should typically be employed for users who need port access only to a particular set of devices or target servers and systems.

New 3.0 Features

These administrator features are now available in CC-SG 3.0:

Note: If viewing a PDF file, click on the page number to navigate to the location in the document where the feature is described.

FEATURE	LOCATION
Import of Categories, Devices, Ports from CSV File	Page 45
Support for adding IPMI Servers and Generic Devices	Page 51
Support for Encryption in KX Devices	Page 54
Discover Device Enhancement	Page 67
Search for Devices	Page 73
In-band Access for Serial, KVM, and Generic Ports	Page 78, 81, 83
Disconnect Users from Port	Page 74
Search for Users	Page 104
Active Directory Enhancements	Page 115
Query Port Report Enhancements	Page 148
View Stored Report	Page 149
Locked Out Users Report	Page 150
CC-NOC Synchronization Report	Page 151
Modem Configuration	Page 166
SNMP Get/Set Enhancements	Page 175
Enable User Lockout	Page 177
Saving MPC Profile Changes	Page 178
CC-NOC Integration Enhancements	Page 181
Scheduling Tasks (Task Manager)	Page 191
Notification Manager	Page 191
Maintenance Mode	Page 159
SSH Access to CC-SG	Page 198
Diagnostic Console	Page 204

New CC-SG 3.0 user features including Port Chat, Bookmark Port, and Search for Ports are documented in Raritan's **CommandCenter Secure Gateway User Guide**.

Chapter 2: Accessing CC-SG

Once you have configured CC-SG with an IP address and have defined at least one user, as described in Raritan's **CommandCenter Secure Gateway Setup Guide**, the CC-SG unit can be placed at its final destination. Make all necessary hardware connections to make the unit operational.

You can access CC-SG in several ways, each described in this chapter:

- Through a browser: CC-SG supports numerous Web browsers (please see the Compatibility Matrix on <http://www.raritan.com/support> and click Firmware Upgrades then CommandCenter for a complete list of browsers and platforms).
- Through a standalone client: Install the executable from the included CD and run this instead of using the browser-based applet. This executable functions exactly like the downloaded applet.
- Through SSH: Please note that remote devices connected via the serial port can be accessed using this approach. Please see **Chapter 12: Advanced Administration** for additional information.
- Through the Diagnostic Console: Provides emergency repair and diagnostics only and is not a replacement for the primary GUI to configure and operate the CC-SG unit. Please see **Chapter 12: Advanced Administration** for additional information.

Note: Users can be connected simultaneously, using the browser, standalone client, and SSH while accessing the application.

Browser-Based Access

1. Using a supported Internet browser, enter the URL of the CC-SG: `https://<IP address>` (for example, `https://10.0.3.30`). When the security alert window appears, click **Yes** to continue with the procedure. CC-SG is always SSL enabled; when you connect via IE, the Security Alert is displayed because the CA root certificate is not installed in the browser.

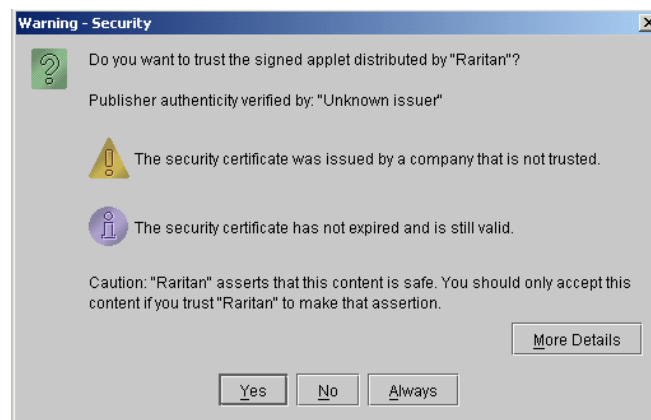


Figure 3 Security Alert Window

2. You will be warned if you are using an unsupported Java Runtime Environment version on your machine. From the window that pops up, select whether you will download the correct JRE version from the CC-SG server (if available), download it from the Sun Microsystems web site, or continue with the incorrect version, and click **OK**. The Login window appears.



Figure 4 Login Window

3. Type your **Username** and **Password** and click **Login**.
4. Upon valid login, the CC-SG application window appears. The menu bar and tool bar, which contain commands for operating and configuring CC-SG, are at the top of the screen. The Ports tab, Users tab, and Devices tab, which contain the Ports selection tree, Users selection tree, and Devices selection tree, appear on the left side of the window. The central panel is where operations and configuration screens will appear.

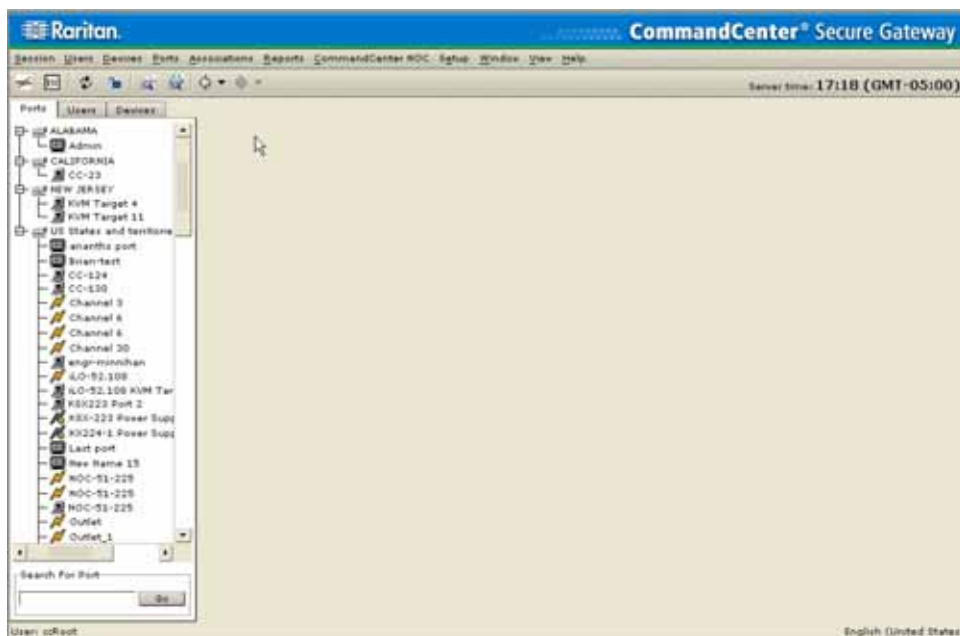


Figure 5 CC-SG Application Window

Standalone Client Access

The standalone CC-SG client allows you to connect to CC-SG servers by launching a Java application instead of running an applet through a Web browser.

1. Install the standalone CC-SG client located on the included CD ROM onto your PC.
2. Double-click on the **CC Application** icon on your desktop to launch the CC-SG client. An address specification window appears.

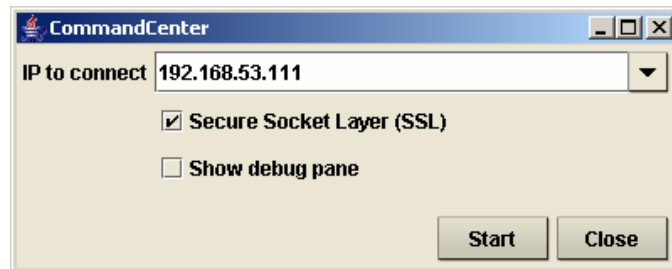


Figure 6 IP Specification Window

3. Type the IP address of the CC-SG unit you wish to access in the **IP to Connect** field and press **Start**. You will be warned if you are using an unsupported Java Runtime Environment version on your machine. Once you have connected to a CC-SG server, its IP address is automatically saved in the client's History file and can be selected from the drop-down menu in the future.
4. After the standalone client successfully connects to CC-SG, the standard login menu appears, and the client looks and behaves just like its browser-based counterpart. Type your **Username** and **Password** and click on **Login** to proceed.

Confirm IP Address

After logging in, you should confirm the IP address, and check firmware and application versions.

1. From the **Setup** menu, click **Configuration Manager**. The **Network Setup** screen should be visible; if not, click on the **Network Setup** tab.

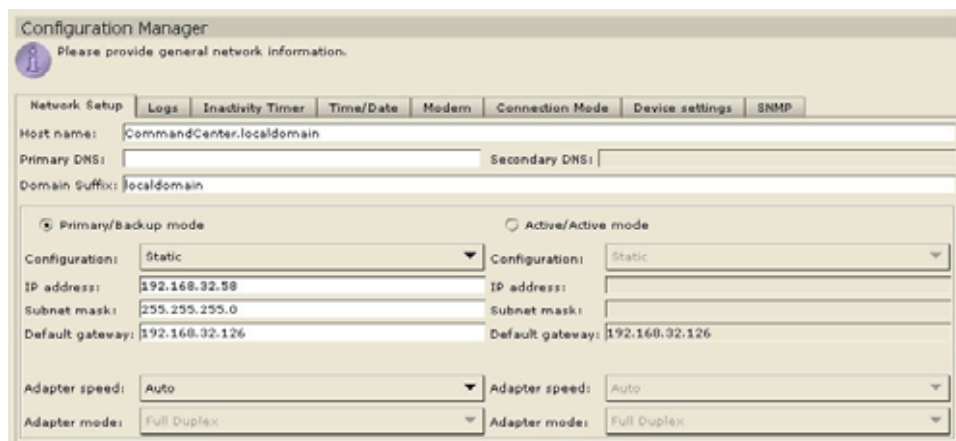


Figure 7 Set IP Address with Configuration Manager Commands

2. Ensure that the network settings display the values entered while setting up the unit; if not, please modify and follow the steps below.

3. Click **Update Configuration** to submit the changes. A confirmation window asks if you wish to restart CC-SG in order to apply changes.
4. Click **OK** to log out from your current session and restart CC-SG.
5. Access CC-SG using the new IP address.

Check and Upgrade CC-SG Firmware Version

Note: Before you can upgrade CC-SG, you must be in Maintenance Mode. See section **Maintenance Mode in Chapter 11: System Maintenance** for additional information.

1. Log onto CC-SG.
2. On the Help menu, select **About Raritan CommandCenter**.
3. If the version is not current, you must upgrade your firmware by following the next few steps.
4. On the **Setup** menu, click **Upgrade CommandCenter**.



Figure 8 Upgrade CC-SG

5. Click **Browse** and locate the file. The file must be accessible from your client PC. This means that it must have been downloaded from the Raritan website or off a Raritan CD.

If you have just acquired the firmware as a zip file, unzip the file and follow the instructions provided by the README file.

Check and Upgrade Application Versions

Check and upgrade the CC-SG applications, for example, Raritan Console (RC) or Raritan Remote Client (RRC).

1. On the **Setup** menu, click **Application Manager**.

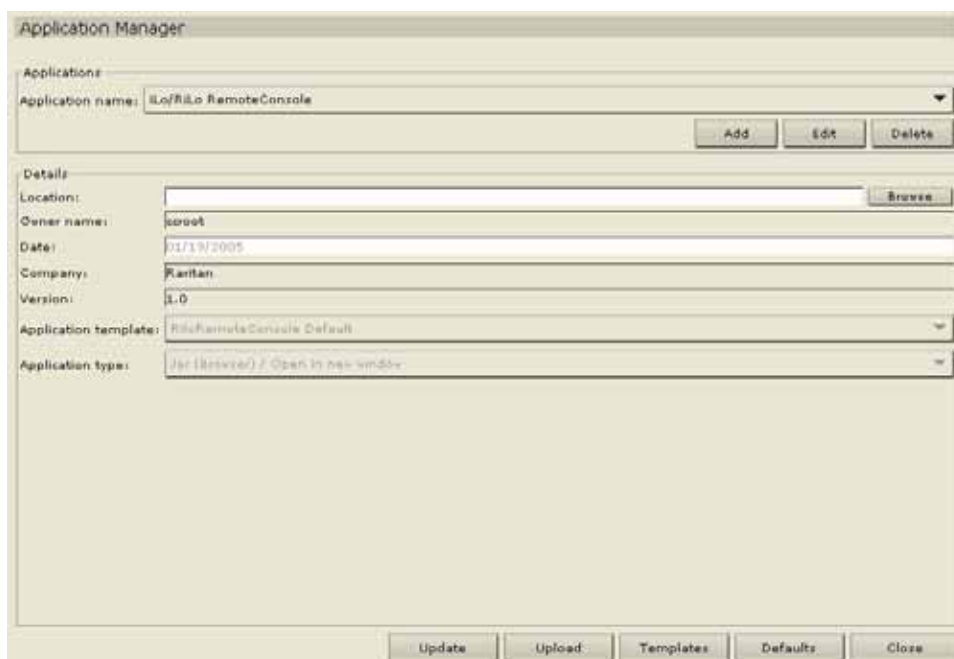


Figure 9 CC-SG Application Manager

2. Select an application from the pull-down menu and note the number in the version field. If the firmware needs upgrading, see the previous section **Check and Upgrade CC-SG Firmware Version** and continue to step 3.
3. Select the application name that needs to be upgraded.
4. Click **Browse**.

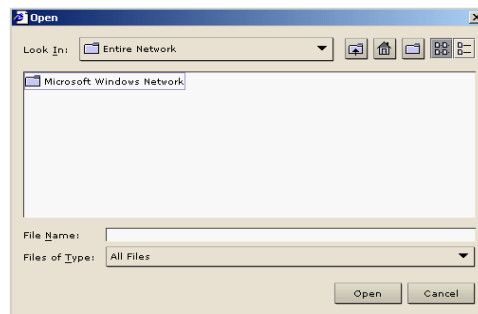


Figure 10 CC-SG Application Search Window

5. Click on the **Look In** drop-down menu and navigate to locate the application on your PC where the new firmware resides. When you find the application, select it, and click **Open**. The application name will appear in the **Location** field in the **Application Manager** screen.
6. Click **Upload** to upload the application. A progress window indicates that the new application is being uploaded. When complete, a new window will indicate that the application has been added to the CC-SG database and is available for configuration and attachment to a specific port.
7. Edit the version field to reflect the new version uploaded, and then click **Update**.
8. Click **Close** to close the **Application Manager** screen.

Connection to Console and KVM Management Appliances

- CC-SG may interface with the Console and KVM management appliances of the Dominion series and the IP-Reach series. Both serial and KVM devices are supported.
- Raritan provides a standard console access, a vt100 Java terminal emulation for remote target devices that require a serial connection. In addition, Raritan offers a variety of specialized applications that allow users to set up a customized look and feel.
- The application interface varies, depending on device type selected. In the case of the KVM device, Raritan provides the complete keyboard, video, and mouse (KVM) of the remote target system through CC-SG.
- CC-SG can also interface with HP servers that have iLO or RILOE access capabilities. In this case, CC-SG will launch HP's own Java management applet when connecting to these devices and log into iLO/RILOE without prompting the user to re-authenticate.

To access a remote target device that is connected via a serial port, click on the appropriate device in the Devices selection tree, under the Devices tab. If the port is configured for a console application, a Security Warning appears, indicating that the console applet is a signed applet from Raritan Systems. Click **Yes** and the console port appears.

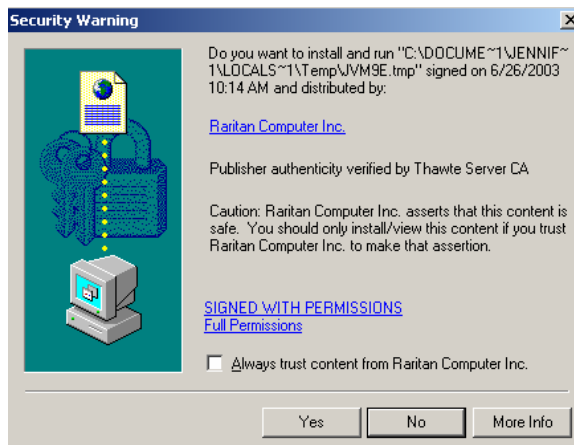


Figure 11 Security Warning for Signed Console Applet

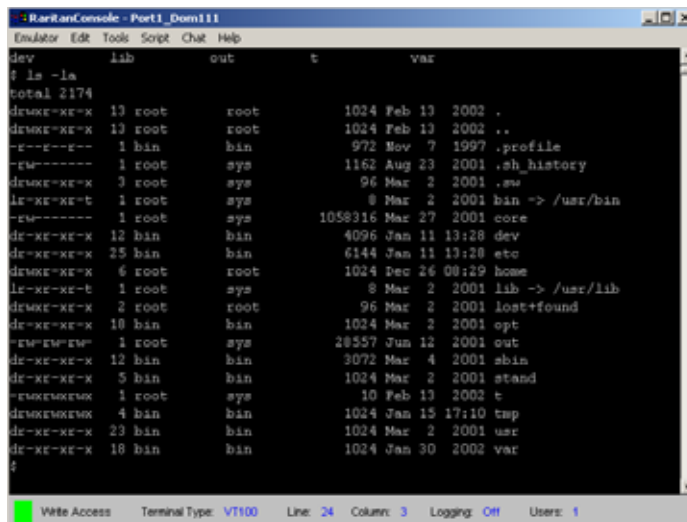


Figure 12 RaritanConsole Application

Warning: The security warning display (appearing in IE only) appears the first time the user connects to a serial port. Click **Yes** when this display appears; if you click **No**, the console application will not launch and you must exit CC-SG, close the browser, re-launch the browser, and connect to CC-SG again.

For additional details about RaritanConsole operation, please refer to Raritan's **RaritanConsole User Guide**.

When a custom application is associated with a KVM or serial port, selecting that port launches the associated application. Raritan Remote Control and RaritanConsole are examples of custom applications that can be integrated into CC-SG.

Power Down CC-SG

If running CC-SG on the V1 platform and if it loses AC power while it is up and running, the V1 unit remembers its last power state. Once AC power is restored, the V1 unit automatically reboots. However, if a V1 unit loses AC power when it is turned OFF, the V1 unit will remain powered off when AC power is restored.

Important: Do not hold the POWER button for four or more seconds to forcibly power down CC-SG, particularly when CC-SG is up and running. The recommended way to power down CC-SG is to use the following procedure.

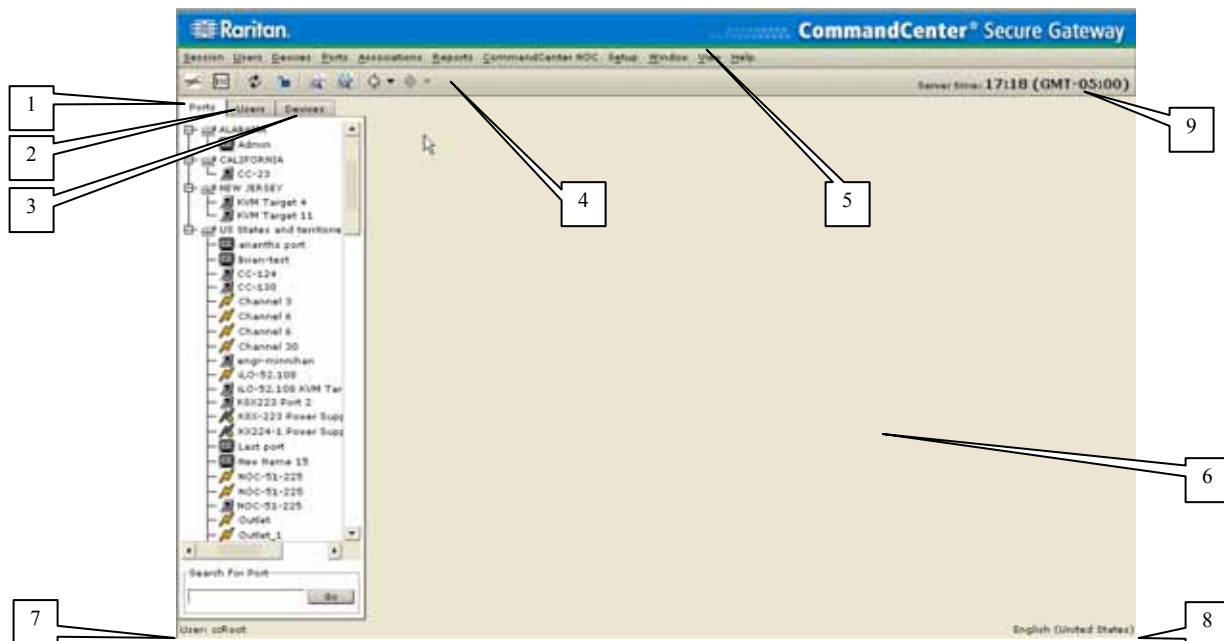
To power down the CC-SG:

1. Remove the bezel and firmly tap the POWER button.
2. Wait for approximately one minute while CC-SG gracefully powers down. You can monitor the progress on the console that is attached to the KVM port.

Note: If users are logged into CC-SG via Diagnostic Console, they will receive a short broadcast message. Users logged into CC-SG via the GUI or SSH will not receive a message.

3. If removing the AC power cord, let the power down process completely finish before removing the power cord. This is required for CC-SG to complete all transactions, close the databases, and place the disk drives into a safe state for power removal.

CC-SG Window Components



1. **Ports Selection tab:** Click on the Ports tab to display all known target Ports in a Ports tree view. Right-click on a port and select **Connect** to connect to that port.
2. **Users Selection tab:** Click on the Users tab to display all registered Users and Groups in a Users tree view. Click on the + and - signs to expand or collapse the tree.
3. **Devices Selection tab:** Click on the Devices tab to display all known Raritan devices in a Devices tree view. Different device types have different icons. Known target ports are grouped under their parent devices, click on the + and - signs to expand or collapse the tree. Right-click on a port and select **Connect** to connect to that port.

Note: To make ports easier to find, right-click on the tree and select the desired listing method under **Port Sorting Options**. Ports sorted by name will be listed alphabetically; ports sorted by status will be grouped in the order of: Available Ports, Busy Ports, Unavailable Ports, and listed alphabetically within each group. On the **Devices** tab, devices are sorted and their respective ports are sorted underneath.

4. **Quick Commands toolbar:** This toolbar offers some shortcut buttons for executing common commands rapidly.

Note: The Quick Commands toolbar includes “Back” and “Forward” buttons, the left and right-pointing arrows. Please use these as you would use the Back and Forward commands in your Internet browser. The Back ← arrow button will return you to the last screen you viewed, and the Forward → button moves you forward to the next screen you viewed, after you have used the Back command.

5. **Operation and Configuration menu bar:** These drop down menus offer commands to operate and configure CC-SG. Please Note: You can also execute some of these commands by right-clicking on the icons in the Ports/Users/Devices tree view.
6. **Main Display area:** The commands you select from the menu bar and/or the tool bar will display in this main area. Displays here are referred to as ‘screens’ and screens may be broken down into ‘panels.’
7. **User ID:** Identification of current logged-in user.
8. **Language Information:** Indication of which language version of CC-SG you are currently using.
9. **Time and timezone** as configured on CC-SG in Configuration Manager. May be different on the client. This time is used when scheduling tasks in Task Manager—see section **Task Manager** in **Chapter 12: Advanced Administration**.

Important: This guide is written to address CC-SG Administrators in the second person. Any phrase that addresses the reader as “you” is referring to users with Administrator privileges. Administrators can assign subsets of Administrator privileges to other users.

Overview

In addition to providing the capability to aggregate and manage multiple Dominion series serial units and IP-Reach units from a central location, CC-SG has powerful built-in features and capabilities for management and configuration:

- Contains administrative tools to manage the application
- Runs health checks on all Dominion and IP-Reach access devices it manages
- Automatically refreshes the Ports, Users, and Devices trees when new components are added
- Queries and sorts information as it is presented on the display
- Configures various authentication schemes, based on operational environment needs
- Allows addition, deletion, and modification of users
- Allows addition, deletion, and modification of Dominion and IP-Reach access devices managed
- Allows addition, deletion, and modification of the applications associated with ports

Main Window Components

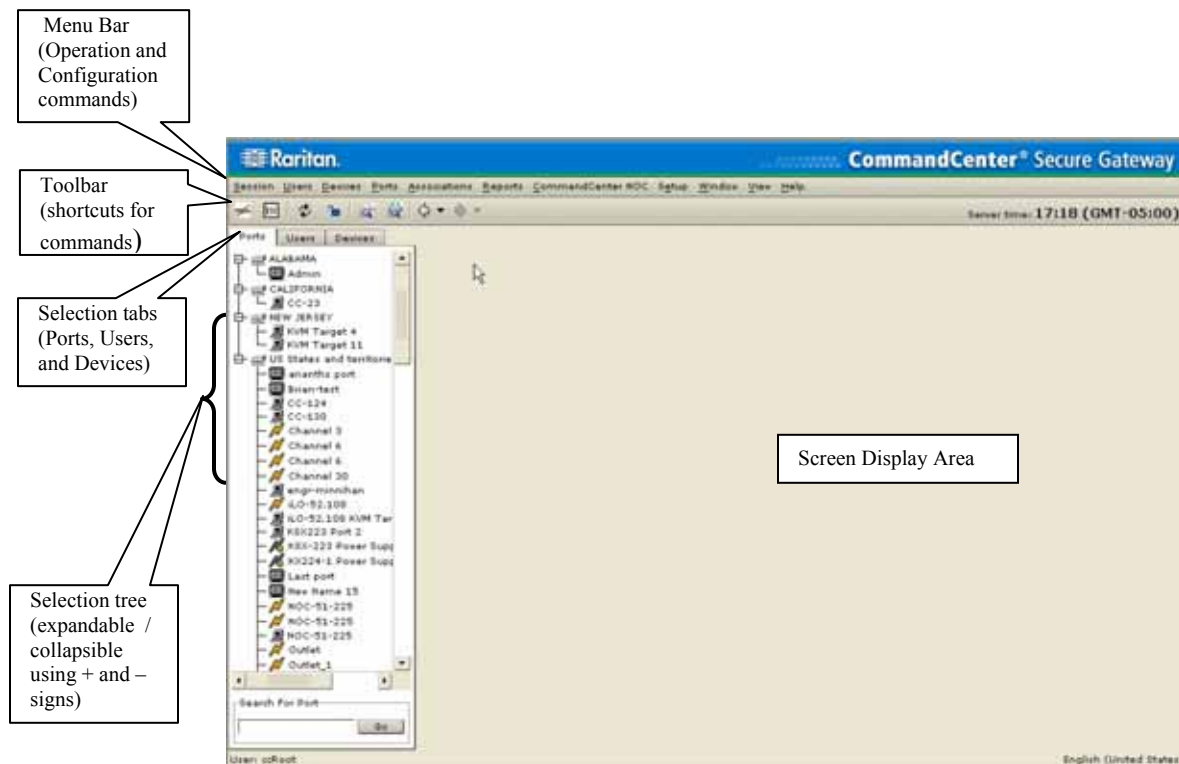


Figure 13 CC-SG Application Window

The CC-SG menu bar displays all operations and configuration commands. Active commands are based upon the privileges of the user, as established by the CC-SG Administrator. The user's privileges also determine the ports and devices that appear in the Ports and Devices trees.

Clicking on the Ports tab displays the Ports selection tree, clicking on the Users tab displays the Users selection tree, and clicking on the Devices tab displays the Devices selection tree. Expand and collapse these trees by clicking on the + and – buttons in front of the icons to view all or a specific set of Ports, Users, or Devices. Users can arrange listed ports by name or status by right-clicking on the tree and selecting the desired **Port Sorting Option**.

Administrators must configure Ports, Users, and Devices in the CC-SG system upon setup and before executing any commands. Please see **Appendix C: Initial Setup Process Overview** for an overview of this process.

Note: The Quick Commands toolbar has been upgraded to include “Back” and “Forward” buttons, the left and right-pointing arrows. Please use these as you would use the Back and Forward commands in your Internet browser. The Back ← arrow button will return you to the last screen you viewed, and the Forward → button moves you forward to the next screen you viewed, after you have used the Back command.

Configuring CC-SG Manager Components

In order to use CC-SG effectively, you must complete the following configuration steps, as described in this and the next chapter:

- Configure and install Dominion series and IP-Reach appliances (both serial and KVM devices).
 - Configure the devices and establish them on your network.
 - Load and associate customized applications for serial ports.
 - Load and associate customized applications for KVM ports.
 - Install and load the KVM client application.
 - Define and configure categories and elements to display the information under the all tabs.
- Create and define users with appropriate privileges and devices they can manage (please see **Chapter 7: Adding Users and User Groups** for additional information).
- Establish the appropriate security and authentication policies. Only an Administrator who has root privileges in CC-SG can do this (please see **Chapter 8: Creating Policies** for additional information).

Configurable Parameters

These fields are mandatory and must follow the guidelines as listed:

User Name: Alphanumeric text, 1 – 16 characters in length, underscores permitted.

Password: Alphanumeric text, 6 – 16 characters in length. The first six characters of the password must contain at least two alpha and one numeric character, and the first four characters cannot be the same as the user name.

Compatibility Matrix

The Compatibility Matrix lists the firmware versions of Raritan devices and software versions of applications that are compatible with the current version of CC-SG. To view the Compatibility Matrix, on the **Devices** menu, click **Compatibility Matrix**.

Compatibility Matrix			
Device:			
Device		Versions	
Dominion SX	3.5		2.4
Dominion KX101	1.0		1.0
Dominion K5X	3.21		3.20
Dominion KX	1.3		4.20
IP-Reach	3.21		3.20
Application:			
Name		Version	
Sun JRE			1.4.2_05
MPG			4.40
Raritan Console			2.7.16
Raritan Remote Client			4.40
You can view latest cross product compatibility matrix online by clicking on the URL below: http://www.raritan.com/support/rup_upgrader.aspx			
			Close

Figure 14 Compatibility Matrix

CC-SG checks against this data whenever you add a device, upgrade device firmware, or select an application for use. If the firmware or software version is incompatible, CC-SG warns you of this before you proceed further.

Note: Each version of CC-SG will only support the current and previous firmware versions for Raritan devices at the time of release.

Chapter 3: Example Configuration Workflow

Create Associations

The Association Wizard guides you through steps to create *categories* and their associated *elements*. The Wizard then automatically creates a port group for each element and a policy for each port group.

1. On the **Associations** menu, click **Association Wizard**. The Association Wizard screen appears.

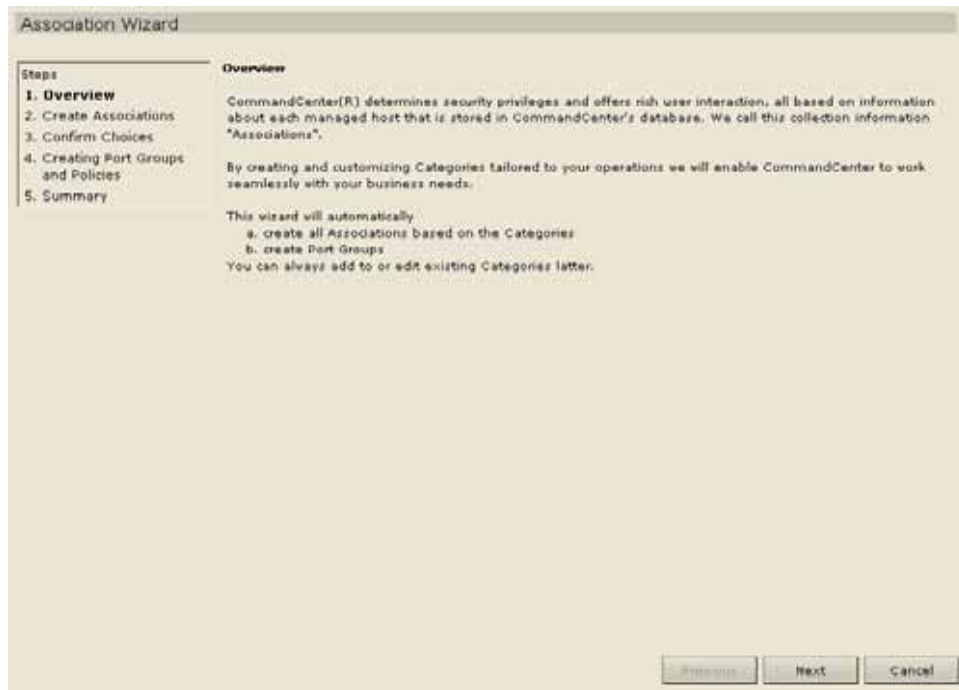


Figure 15 Association Wizard Overview

2. After reading the overview, click **Next**. The **Create Category and Elements** screen of the Wizard appears.

Association Wizard

Steps

1. Overview
2. **Create Associations**
3. Confirm Choices
4. Creating Port Groups and Policies
5. Summary

Create Categories and Elements

Category: Location

Elements:

1. LA Market Area	2. Chicago Market Area
3. New York Market Area	4. Atlanta Market Area
5.	6.
7.	8.

Add More Elements

Previous Add Another

Previous Next Done

Figure 16 Association Wizard - Category and Elements Screen

3. Type the name of a category you wish to organize your ports by (for example: *Location*) in the **Category** field.
4. Type the name of each element in that category in the **Elements** fields below. These elements are used to group your ports within the category (for example: *LA Market Area*, *Chicago Market Area*, etc.). If you require more than eight elements for this category, click **Add More Elements**.

- To create another category, click **Add Another Category** and repeat steps 3 and 4. To review categories and elements you have created, click **Previous** or **Next** to cycle through them.

Association Wizard

Steps

1. Overview
2. Create Associations
3. Confirm Choices
4. Creating Port Groups and Policies
5. Summary

Create Categories and Elements

Category: Function

Elements:

1. Sales Servers	2. Monitoring
3. Production	4. Testing Rack
5. Demo Rack	6.
7.	8.

Add More Elements

Previous Add Another

Previous Next Done

Figure 17 Adding Another Category

- When you are done creating categories, click **Next** at the bottom of the screen. The **Confirm Choices** screen of the Wizard appears.

Association Wizard

Steps

1. Overview
2. Create Associations
3. Confirm Choices
4. Creating Port Groups and Policies
5. Summary

Confirm Choices

The following categories and elements will be created:

Category	Elements
Location	LA Market Area, Chicago Market Area, New York Market Area, Atlanta Market Area
Function	Sales Servers, Monitoring, Production, Testing Rack, Demo Rack

Previous Finish Done

Figure 18 Association Wizard - Confirm Choices

- Review the list of categories and associated elements that will be created. Click **Previous** if you need to go back and make changes. If everything is correct, click **Finish**.

8. CC-SG will show a progress bar while it is creating the associations, port groups and policies. When this is complete, the **Association Wizard Summary** screen appears displaying the list what was created. Click **Done** to exit the wizard.



Figure 19 Association Wizard - Summary Screen

The Association Wizard has now created a port group for each element, and a policy for each port group. You can add ports to these port groups by using the **Port Group Manager**. To make changes to any of the categories after using the Wizard, from the **Associations** menu, click **Association Manager**. To make changes to any of the policies, click **Policy Manager** from the **Associations** menu. By default, the Association Wizard sets the policy for control access at all times.

Add Devices

Before adding devices to CC-SG, prepare them by assigning them an IP address, creating a CC-SG admin account. Please see **CommandCenter Secure Gateway Setup Guide** for more information.

Important: Ensure that no other users are logged into the device during CC-SG configuration.

1. Click on the **Devices** tab.
2. On the **Devices** menu, click **Device Manager**, and then click **Add Device**. The **Add Device** selection screen appears.



Figure 20 Add Device CC-SG

3. Click on the **Device Type** drop-down arrow and select a type of device from the list.

4. Click **Next** to proceed. The **Add Device** description screen appears. Depending on the type of device you selected, you will see slightly different Add Device screens.

Add Device
Please select device properties to add.

Device type: PowerStrip

Device name:

Description:

Number of ports: 8

Category	Element	Apply To Ports
US States and territories		☐

Previous OK Cancel

Figure 21 Add Device PowerStrip

Add Device
Please select device properties to add.

Device type: Dominion SX

Device name:

Device IP or Hostname:

Description:

Username:

Password:

Category	Element	Apply To Ports
US States and territories		☐

Previous OK Cancel

Figure 22 Add Device SX

5. Type the device name in the **Device Name** field. Do not use spaces.
6. Type the device description in the **Description** field.
7. Type the **Device IP** address when you prepared the device and use the previously created CC-SG **Username** and **Password**, such as **ccadmin/password**. Please see Raritan's **CommandCenter Secure Gateway Setup Guide** for additional information.
8. Select a category and appropriate element from the **Category and Element** (double-click on an element field to see and select element choices) window. Click **OK** to add the device. A

Device Created successfully message confirms that device has been added. This step is very important. Make sure you select the correct associations and elements for the device. Some devices such as SX may take up to a minute to add.

- Repeat steps 1 through 8 to add additional devices.

Configure Ports

You must now add ports for each device you just added. The port is the connection to the actual target system or server. After adding ports, you can change the configuration of individual ports by clicking the **Ports** tab, right-clicking on a port, and clicking **Edit Port**.

Serial Port

- Click on the **Devices** tab and select a serial device, for example, Dominion SX, from the Devices tree.
- On the **Devices** menu, click **Port Manager**, and then click **Configure Ports**. Alternatively, you can right-click on the device and select **Configure Ports**. The **Configure Ports** screen appears.

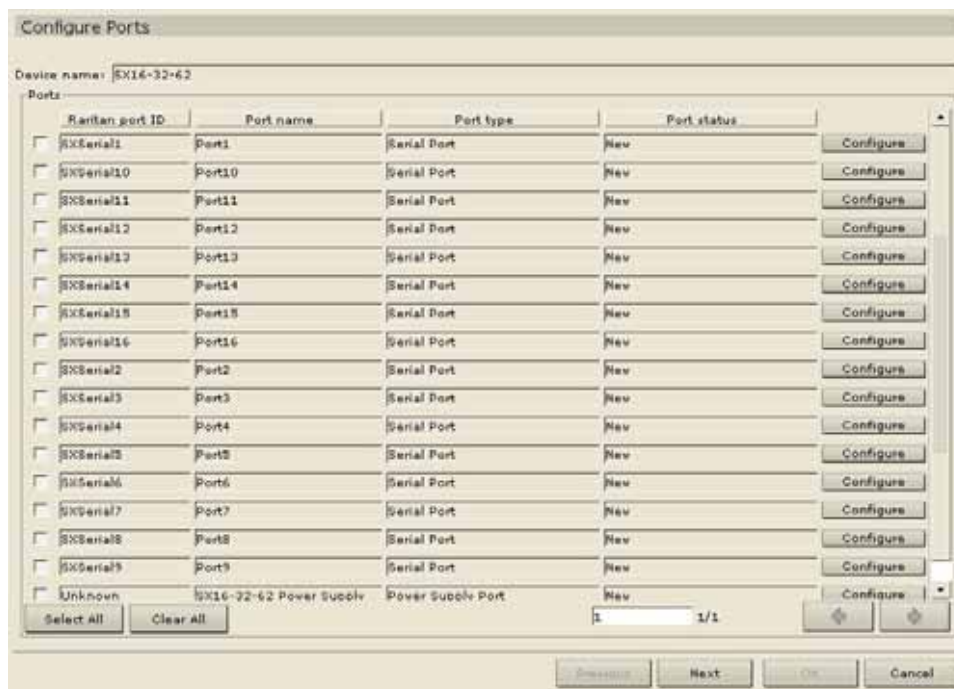


Figure 23 Configuration Ports

- Click **Configure** next to the serial port line item you wish to configure. The **Configure Serial Port** screen appears.

Configure Serial Port

Please select port properties to add.

Device name: 0K16-32-62

Device IP or Hostname: 192.168.32.62

Port number: XXSerial1

Port name: Port1

Application name: RaritanConsole

Baud rate: 9600

Parity/Data bits: None/8

Flow control: None

Associate power strip: None

Category	Element
System Type	US States and territories

OK Cancel

Figure 24 Configure Serial Ports

- Type a port name in **Port Name** field. Typically, you should name the port after the target server the device connects to, for example, **NYC_MsSrv1**.
- Click on the **Application Name** drop-down menu and select an application name. This application, for example, Raritan Console (RC), is used to manage the target system.
- Click on the **Baud Rate** drop-down arrow and select a rate.
- Click on the **Parity/Data Bits** drop-down arrow and select a parity value.
- Click on the **Flow Control** drop-down arrow and select a flow control value.
- Click on the **Associate Power Strip** drop-down arrow and associate with a power strip if necessary.
- Select the associated category and element from the **Port Associations** table by double-clicking the element field.
- Click **OK** to save the serial port configuration. A **Port Configured Successfully** message confirms that port has been created.
- Repeat steps 1 through 11 to configure other serial ports.

KVM Port

1. Click on the **Devices** tab and select a KVM device, for example, Dominion KX, from the Devices tree.
2. On the **Devices** menu, click **Port Manager**, and then click **Configure Ports**. Alternatively, you can right-click on the device and select **Configure Ports**. The **Configure Ports** screen appears.

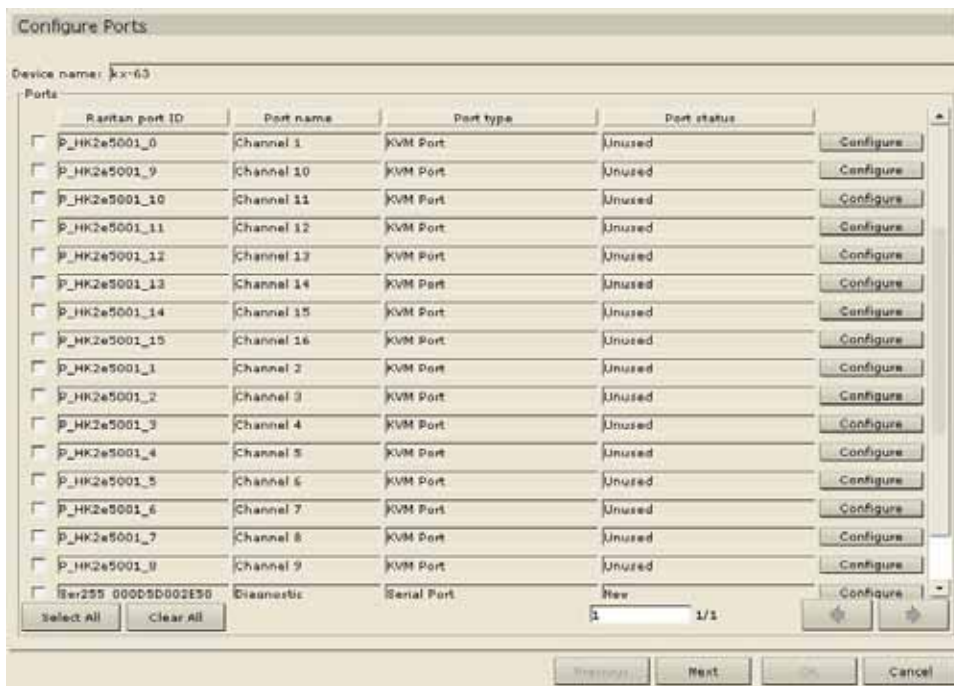


Figure 25 Configure Ports

3. Click **Configure** next to the KVM port line item you wish to configure. The **Configure KVM Port** screen appears.

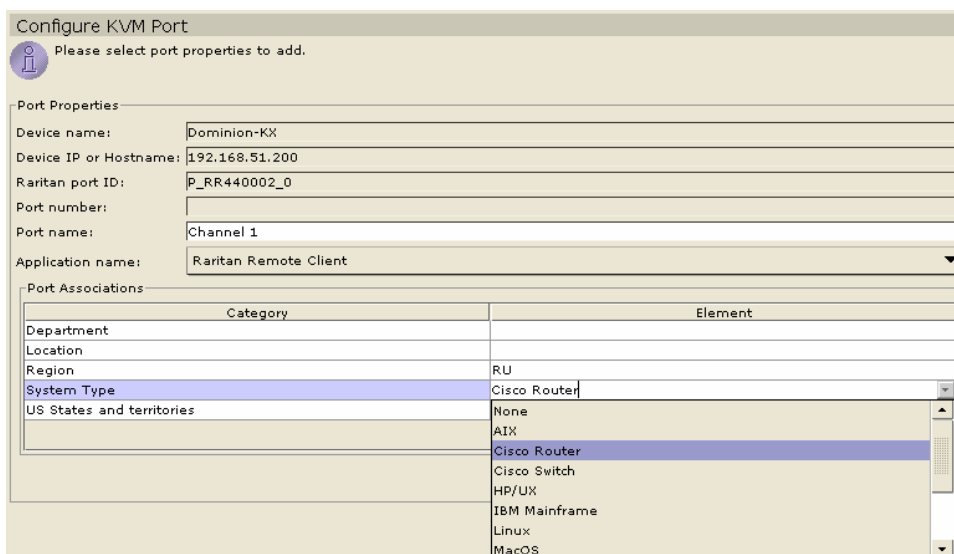


Figure 26 Configure KVM Port

4. Type a port name in the **Port Name** field. Typically, you should name the port after the target server the device connects to, for example, **NYC_MsSrv1**.

5. Click on the **Application Name** drop-down menu and select name. This application, for example, Raritan Remote Console (RRC), is used to manage the target system. All ports should use RRC except for those on an SX.
6. Select the associated category and element from the **Port Associations** table by double-clicking the element field.
7. Click **OK** to save the KVM port configuration. A **Port Configured Successfully** message confirms that port has been created.
8. Repeat steps 1 through 7 to configure other KVM ports.

Add Users to System Administrators Group

If you want your users to have access to all devices, ports, and CC-SG, you can simply create and place users in the System Administrators user group. This simplifies the configuration process by eliminating the need to create user groups, port groups, and policies to control user access. If you do not put users in the default System Administrators group, you will need to complete the additional sections that follow this one. After adding a user, they will be able to log into CC-SG and connect to ports, configure the system, etc.

Note: Please remember that many of the commands in the **Users** menu can be accessed by right-clicking on the user icon and using the shortcut menu that appears.

1. Click on the **Users** tab.
2. On the **Users** menu, click **Add User**. Alternatively, right-click on a user and select **Add User**. The **Add User** screen appears.

Figure 27 Add User Screen

3. Type the user's name in the **Username** field (1-32 characters, alphanumeric characters or underscores, no spaces).
4. Check the **Remote Authentication** check box only if the user should be authenticated by TACACS+, RADIUS, LDAP, or AD. **Note:** Checking the **Remote Authentication** box implies that a remote server is being used for authentication. If so, a local password is not needed and the **Password** and **Retype Password** fields are grayed out.

5. If using local authentication, type the new password into the **Password** field (6-16 characters, alphanumeric characters and underscores).
6. If using local authentication, re-type password in **Retype Password** field.
7. Type a dial back number in the **Dial Back Number** field, if needed.
8. Check the **Login Enabled** check box to authenticate against the system (if not, user cannot enter the system).
9. Check the **Force Change Password on Next Login** check box if you want this user to be forced to change password the next time he or she logs in to CC-SG.
10. Check the **Force Change Password Periodically** check box if you want this user to have to change his or her password from time to time.
11. Type the expiration period for this user's password in the **Expiration Period** field.
12. Type an email address for this user in the **Email Address** field, if desired.
13. Click **OK** to add this user to the system. A **User Created successfully** message indicates the user has been added to the system.
14. Drag the new user icon to the desired user group.
15. Repeat steps 1 through 14 to add additional users.

Important: If you do not wish to restrict or control user access to systems or CC-SG, your installation is now complete. Your users should all be assigned to the system administrator's user group.

Control User Access

You can control user access to devices, ports, and CC-SG administration through *user groups* and *policies*. User groups define a user's privileges and policies specify the devices and ports a user can access. First, create a user group, apply a policy to the user group, then add users to the user group.

Create User Groups

Use the **Add User Group** command to create specific user groups and assign them privileges, based on the needs of your work environment. Groups can help you keep your system organized.

Assign privileges to Groups upon creating them. These privileges are either a command type or an event type. Command type privileges permit users to see and execute commands. Event type privileges permit users to view events in the Ports and Devices trees.

Users inherit the privileges assigned to the group to which they belong. No user can have any rights other than those assigned to the group. As an example, if a group is assigned the **User Management** privilege, all users in that group can see and execute the User Manager commands in the **Users** menu: **Add User**, **Edit User**, **Change User Password**, etc.

In order to see Ports and Devices trees, a user group has to be assigned the **Device and Port Management** privilege. To view other events that occur in the system, those privileges must be selected upon adding or editing a user group.

Note: A user group by default has no access to any ports. Therefore, a policy must be applied to the user group.

1. Click on the **Users** tab.

2. On the **Users** menu, click **Add User Group**. Alternatively, right-click on a user group and select **Add User Group**. The **Add User Group** screen appears.

Add User Group
Choose usergroup properties to add.

User group name:

Description:

Select Privileges

Has It	Name	Type
☐	CC Setup And Control	Command
☐	Device And Port Management	Command
☐	Device Configuration And Upgrade Management	Command
☐	Ports Access	Command
☐	CC Configuration	Event
☐	CCConnectionManagement	Event
☐	DeviceGroupManagement	Event
☐	DeviceManagement	Event
☐	PortGroupManagement	Event
☐	PortManagement	Event
☐	UserGroupManagement	Event
☐	UserManagement	Event

OK Cancel

Figure 28 Add User Group Screen

3. Type the group name in the **User Group Name** field (1-16 characters, alphanumeric characters and underscores).
4. Type the group description (for example, based on department, region, or assignment) in the **Description** field.
5. In the **Select Privileges** section, check the corresponding boxes in the **Has it** column to add those privileges to the group. The **Type** column indicates whether the privilege is a Command type or Event type. Most user groups should only have **Ports Access** enabled to allow them to access systems and servers.
6. Click **OK** to add the group. A **Group Created Successfully** message confirms that a group has been created.
7. Repeat steps 1 through 6 to add other groups.

Create/Edit Port Groups

CC-SG uses port groups to control user access. Policies can be applied to specific user groups that allow only access to those ports specified in the port group. For example, if you wanted to restrict user access to only UNIX ports, you would create a port group that included only UNIX ports. Then you would create a policy that included this port group and apply it to the desired user group.

Port groups were automatically created per element when the Association Wizard was run, see **Create Associations** earlier in this chapter for additional information. These port groups contain general rules so you may want to edit these port groups and add more specific rules.

1. On the **Associations** menu, click **Groups Manager** and then click **Port Group Manager**. The Port Groups Manager screen appears.

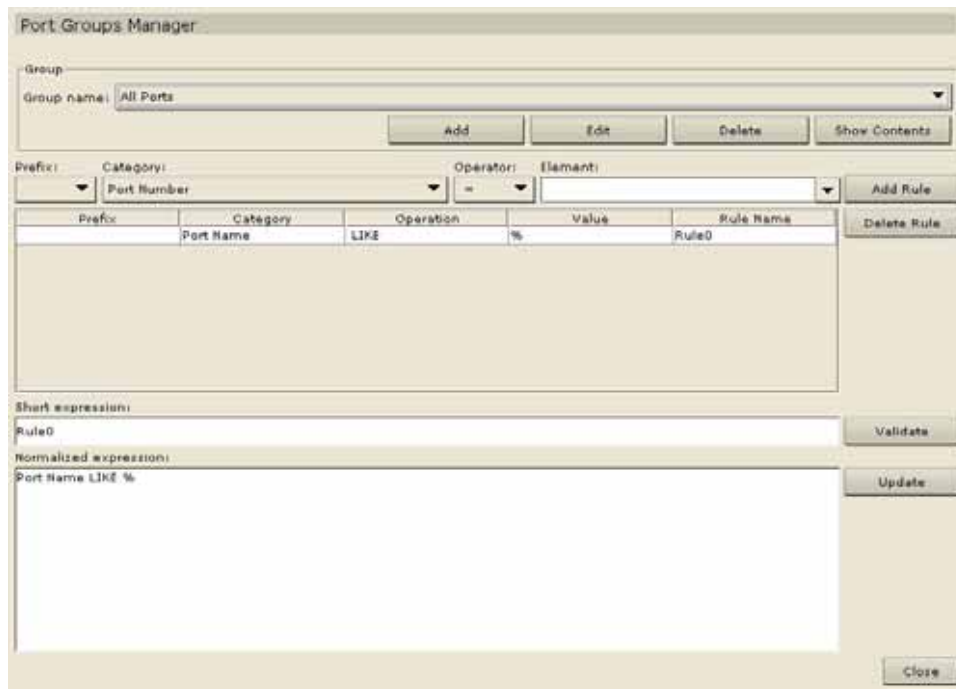


Figure 29 Port Groups Manager Screen

2. Click **Add** in the **Group** panel to add a new group. The **Add Port Group** window appears.



Figure 30 Add Port Group Window

3. Type the name for the new Port Group in the **Enter Port Group Name** field.
4. Click **OK** to add the new group.
5. Create a desired rule (such as PortType=UNIX) using pre-defined categories and elements and then click **Add Rule**. In this example, PortType is a category and UNIX is an element. Repeat for additional rules.

6. If needed, enter the Boolean logic to apply additional rules in the **Validate** panel. Example: use (Rule0 & Rule1) for AND or use (Rule0 | Rule1) for OR. Additional combinations can be used.
7. Click **Validate** then **Update**.
8. Click **Close** to close Port Groups Manager screen.
9. Repeat steps 1 through 8 to add other port groups.

Create/Edit Policies

Policies specify the devices and ports a user can access as well as when they can be accessed. Policies were automatically created per element when the Association Wizard was run, see section **Create Associations** earlier in this chapter for additional information. These policies, for example, Allow Linux Ports, include the port group that was automatically generated and grant full access to the ports. Once created, you will then apply the policy to a user group.

1. On the **Associations** menu, click **Policy Manager**. The **Policy Manager** screen appears.

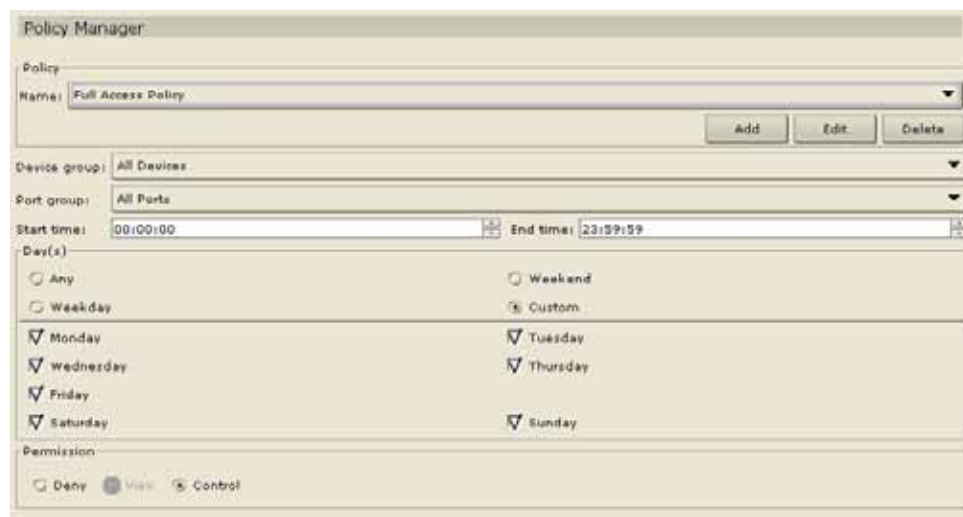
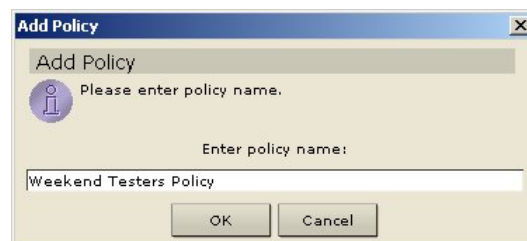


Figure 31 Policy Manager Screen

2. Click **Add** to add a new policy. The **Add Appliance Policy** window appears.



3. Type the name of the new policy in the **Enter Policy Name** field.
4. Click **OK** to add the new policy. If you clicked **OK**, the new policy name appears in the **Name** field.
5. Click on the **Device Group** drop-down arrow and select a device group.
6. Click on the **Port Group** drop-down arrow and select a port group.
7. Click on the up or down arrows in the **Start Time** and **End Time** fields to assign a starting time and an ending time during a 24-hour period for this policy to be in effect.
8. Select the appropriate option buttons for this policy to be in effect: **Any** to apply policy every day, **Weekday** to apply policy every working day, **Weekend** to apply policy Saturdays and

Sundays, and **Custom** to manually choose the days policy to be applied. If you choose **Custom**, check on the days of the week to apply the policy.

9. Click on a **Permission** value to select a permission type: **Deny**, or **Control**.
10. Click **Update** to add the policy. The **Update Policy** window appears.

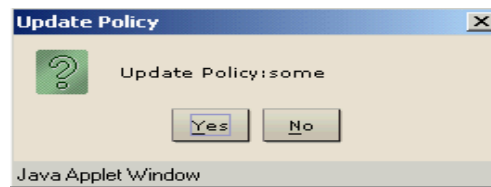


Figure 32 Update Policy Window

11. Click **Yes** to add the policy or **No** to close the window.
12. Click **Close** to close the **Policy Manager** screen.
13. Repeat steps 1 through 12 to add other policies.

Apply Policies to User Groups

A user group does not specify the ports that can be accessed by the group and a policy does. Therefore, you need to apply a policy to a user group.

1. Click on the **Users** tab and select a group.
2. On the **User** menu, click **Edit User Group Policies**. Alternatively, right-click on a user group and select **Edit User Group Policies**. The **Edit User Group Policies** screen appears.

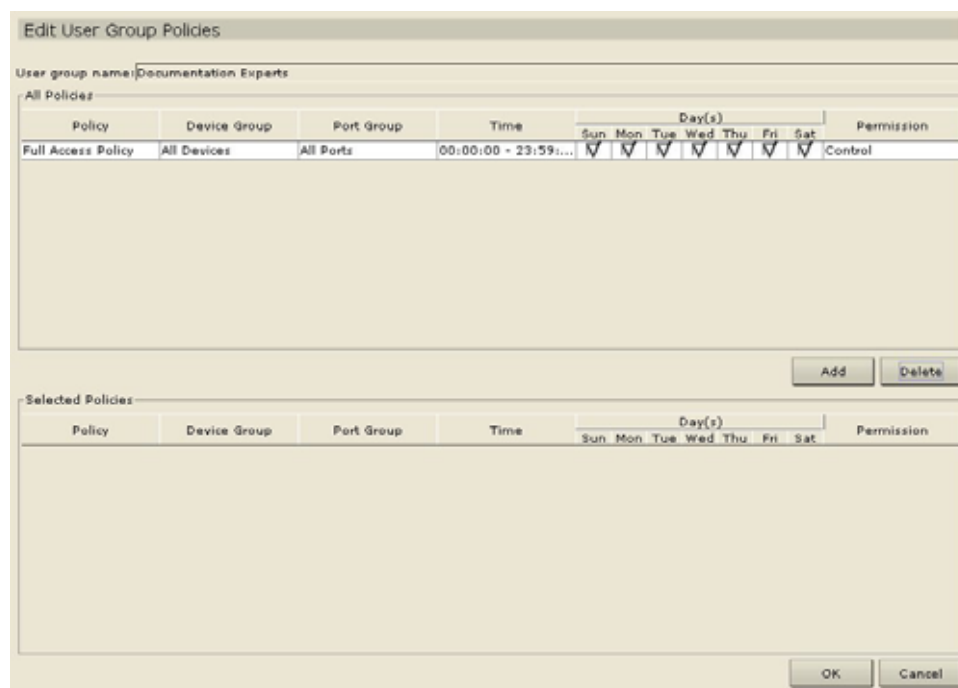


Figure 33 Edit User Group Policies Screen

3. Scroll up or down to view all policies in this list. Click on a line item in the **Policies** list (under the **All Policies** panel) that you wish to assign to the group. Click on the **Day(s)** check boxes to select which days of the week the policy should be assigned.
4. Click **Add** to add the policy to the **Selected Policies** panel and assign it to the group.
5. To remove an assigned policy from the **Selected Policies** list, select the policy line item and click **Delete**.

6. Click **OK** to add the policy or policies to the group. A **Group Policies Updated successfully** message confirms that policies have been updated.
7. Repeat steps 1 through 6 to edit other groups' policies.

Add Users to User Group

You now need to add users or drag and drop an existing user to the user group that has just been assigned a policy. These users will then be able to login to the CC-SG and have access or be denied access to the ports as specified in the policy.

1. Click on the **Users** tab and select the user group you wish to add the user to.
2. On the **User** menu, click **Add User**. Alternatively, right-click on a user and select **Add User**. The **Add User** screen appears.

Figure 34 Add User Screen

3. Type the user's name in the **Username** field (1-32 characters, alphanumeric characters or underscores, no spaces).
4. Check the **Remote Authentication** check box only if the user should be authenticated by TACACS+, RADIUS, LDAP, or AD. **Note:** Checking the **Remote Authentication** box implies that a remote server is being used for authentication. If so, a local password is not needed and the **Password** and **Retype Password** fields are grayed out.
5. If using local authentication, type the new password into the **Password** field (6-16 characters, alphanumeric characters and underscores).
6. If using local authentication, re-type password in **Retype Password** field.
7. Type a dial back number in the **Dial Back Number** field, if needed.
8. Check the **Login Enabled** check box to authenticate against the system (if not, user cannot enter the system).
9. Check the **Force Change Password on Next Login** check box if you want this user to be forced to change password the next time he or she logs in to CC-SG.
10. Check the **Force Change Password Periodically** check box if you want this user to have to change his or her password from time to time.
11. Type the expiration period for this user's password in the **Expiration Period** field.

12. Type an email address for this user in the **Email Address** field, if desired.
13. Click **OK** to add this user to the system. A **User Created successfully** message indicates the user has been added to the system.
14. Drag the new user icon to the desired user group.
15. Repeat steps 1 through 14 to add additional users.

Chapter 4: Creating Associations

Associations

CC-SG provides powerful, highly customizable organizational capabilities. Associations provide this organizational capability and are used to organize your equipment. For example, you may have Raritan devices that manage target servers in a New York data center and a Philadelphia data center. Associations help in grouping and displaying Raritan device and target systems in the CC-SG web interface. For example, the following screen is a custom view that hierarchically displays three data centers, that is, DataCenter1, NYC, and Philadelphia, and the type of target servers in them. You can customize the CC-SG to organize and display your servers however you like.

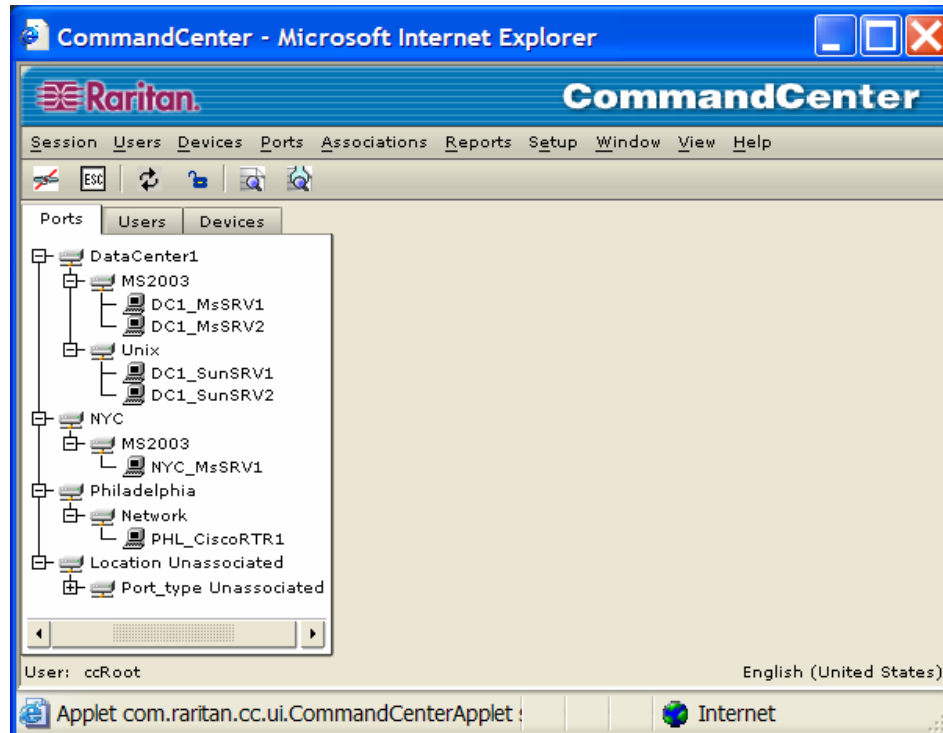


Figure 35 CC-SG Organization Example

Associations-Defining Categories and Elements

An important concept in CC-SG is *categories* and *elements*. Categories and elements are defined with the Association Wizard or Association Manager. Raritan devices and ports are organized by category and elements. Each category/element pair is assigned to a device, a port, or both. Therefore, you need to define your categories and elements before you add a Raritan device and configure ports in CC-SG.

A category is a group, or set, of similar elements. For example, you could have a category to group your Raritan devices by location. So, Location, can be a category and could contain a set of elements, such as New York City and Philadelphia. These organizational capabilities are defined using the Association Wizard or Association Manager.

The categories and elements are also used by policies, which are used to control user access to servers. The above example can be used to create policies to control user access to only NYC servers, or network ports, or any combination such as MS2003 servers in NYC.

Other examples of typical Association configurations of Category and Elements are as follows:

CATEGORY	ELEMENTS
Location	New York City, Philadelphia, DC1
OS Type	Unix, Windows, Linux
Department	Sales, IT, Engineering
Port Type	KVM, Serial, Power

Association configurations should be kept simple to accomplish server/port organizational objectives and user access objectives. It is important to realize that a port can only be assigned to a single element of a category. For example, a target server cannot be assigned to both the Windows and Unix elements of the OS Type category above.

A useful approach for organizing your systems when servers are similar and need to be randomly organized is the following:

CATEGORY	ELEMENT
usergroup1	usergroup1port
usergroup2	usergroup2port
usergroup3	usergroup3port

The design and specification of the Association requirements should be done prior to setting up CC-SG. You should give careful thought upfront on how you want to organize and display your Raritan devices and target systems and how you want to control user access to the ports.

As you add devices and ports, you link them to your predefined categories and elements. When you create port and device groups to include in a policy, you will use your categories and elements to define which ports and devices go in each group.

Association Terminology

You should read the following definitions to understand associations:

- **Associations**—is the relationship between categories, elements of a category, and ports or devices or both. For example, you want to associate the “Location” category with a device. You should create associations first, or edit them later, before adding devices and ports in CC-SG.
- **Category**—is a variable that contains a set values or elements. An example of a Category is Location, which may have elements such as “New York City”, “Philadelphia”, or “Data Center 1”. When you add devices and ports to CC-SG, you will associate this information with them. It is easier if you set up associations correctly first, before adding devices and ports to them. Another example of a Category is “OS Type”, which may have elements such as “Windows” or “Unix” or “Linux”.
- **Elements**—are the values of a category. For example, the “New York City” element belongs to the “Location” category. Or, the “Windows” element belongs to the “OS Type” category.

- **Devices**—are Raritan products such as Dominion KX116, Dominion SX48, Dominion KSX440, IP-Reach, Paragon II System Controller, Paragon II UMT832 with USTIP, etc. that are managed by CC-SG. These devices control the target servers and systems that are connected to them.
- **Ports**—are connection points between a Raritan Device and a target system or server. Or, a port can be a device that is directly connected to a LAN/CC-SG via In-band access. In CC-SG, you click on a port to access and manage the target. The port is essentially the destination system and should be named appropriately for that system, for example, **NYC_SunSRV1**.

How to Create Associations

An easy way to create categories and elements within these categories is by using CC-SG's *Association Wizard*. The wizard prompts you to create categories and elements and automatically creates port groups and default user policies based on the categories and elements defined.

You can also manually create or edit associations with the *Association Manager*. This will require you to manually create policies.

Association Manager

Association Manager commands allow you to add, modify, or delete Categories and Elements. In CC-SG, each device or port has an associated IP Address and Port Name by default. For further differentiation, additional types of attributes, known as *categories*, are associated to the device or port for ease of administration. Each Category has *elements* associated with it.

For example, the category “Country” might have the elements “USA,” “Japan,” and “Germany” associated with it; the category “Location” might have the elements “San Jose,” “San Francisco,” and “New York” associated with it, and so on. Once the tree view is customized using these attributes, you can easily find, for example, all Firewall devices located in the New York location without searching through an extensive list of managed devices/ports.

Once you add a new category and its elements, you can associate CC-SG's configured devices/ports. When configuring devices/ports, you can choose one element from each category to associate with each device/port.

Please see **Appendix C: Initial Setup Process Overview** for a summary of this process within CC-SG.

Add Category

1. On the **Associations** menu, click **Association Manager**. The **Association Manager** screen appears.

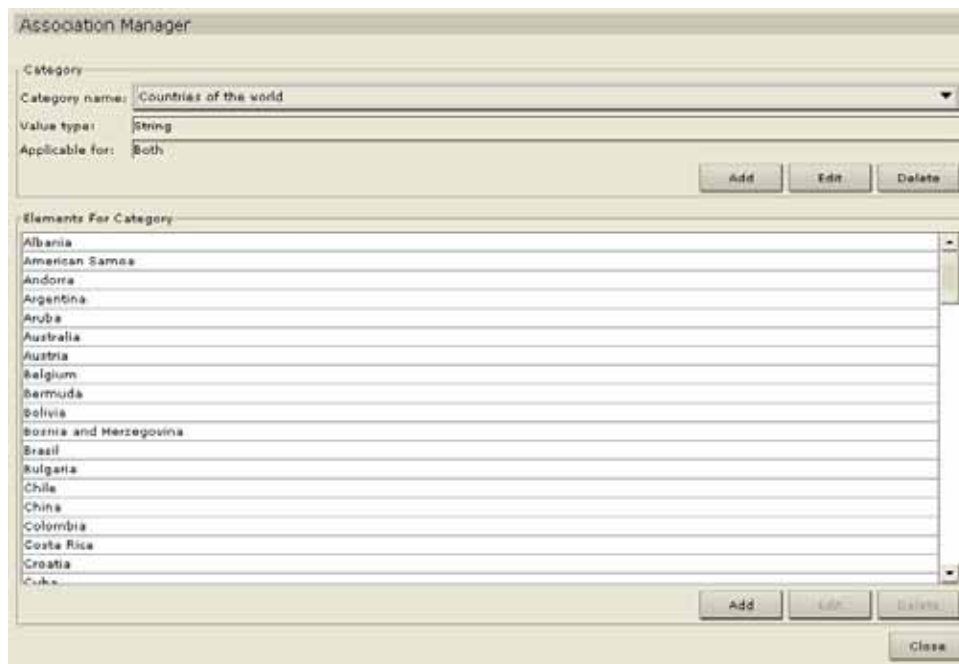


Figure 36 Association Manager Screen

2. Click **Add** in the **Category** panel to add a new category. The **Add Category** window appears.



Figure 37 Add Category Window

3. Type a category name in the **Category Name** field. Maximum length is 31 characters.
4. Click on the **Value Type** drop-down arrow to select a value type of **String** or **Integer**.
5. Click on the **Applicable For** drop-down arrow to select the type of device this category applies to: **Device**, **Port**, or **Both**.
6. Click **OK** to create the new category or **Cancel** to exit without creating. The new category name appears in the **Category Name** field.
7. Repeat steps 1 through 6 to add other new categories.

Edit Category

1. On the **Associations** menu, click **Association Manager**. The **Association Manager** screen appears.
2. Click on the **Category Name** drop-down arrow and select the category to be edited.
3. Click **Edit** in the **Category** panel of the screen to edit the category. The **Edit Category** window appears.



Figure 38 Edit Category Window

4. Type the new category name in **Category Name** field.
5. Click the **Applicable For** drop-down arrow to change whether this category applies to **Device**, **Port**, or **Both**. Please note that a string value cannot be changed to an integer value, and vice versa. If you must make this type of change, please delete the category, and add a brand new one.
6. Click **OK** to edit the category or **Cancel** to exit without editing. The updated category name appears in the **Category Name** field.
7. Click **Close** to close the **Association Manager** screen.
8. Repeat steps 1 through 7 to edit other categories.

Delete Category

Deleting a category deletes all of the elements created within that category. The deleted category will no longer appear in the Devices tree once the screen is refreshed or the user logs out and logs back into CC-SG.

1. On the **Associations** menu, click **Association Manager**. The **Association Manager** screen appears.
2. Click on the **Category Name** drop-down arrow and select the category to be deleted.
3. Click **Delete** in the **Category** panel of the screen to delete the category. The **Delete Category** window appears.

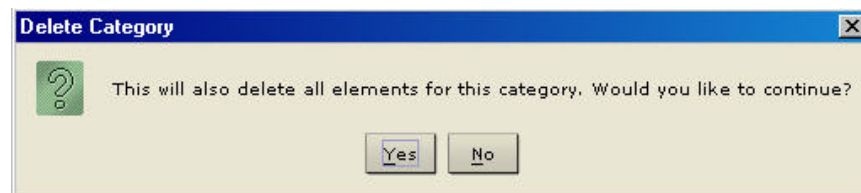


Figure 39 Delete Category Window

4. Click **Yes** to delete the category or **No** to close the window.
5. Click **Close** to close the **Association Manager** screen.
6. Repeat steps 1 through 5 to delete other categories.

Add Element

1. On the **Associations** menu, click **Association Manager**. The **Associations Manager** screen appears.

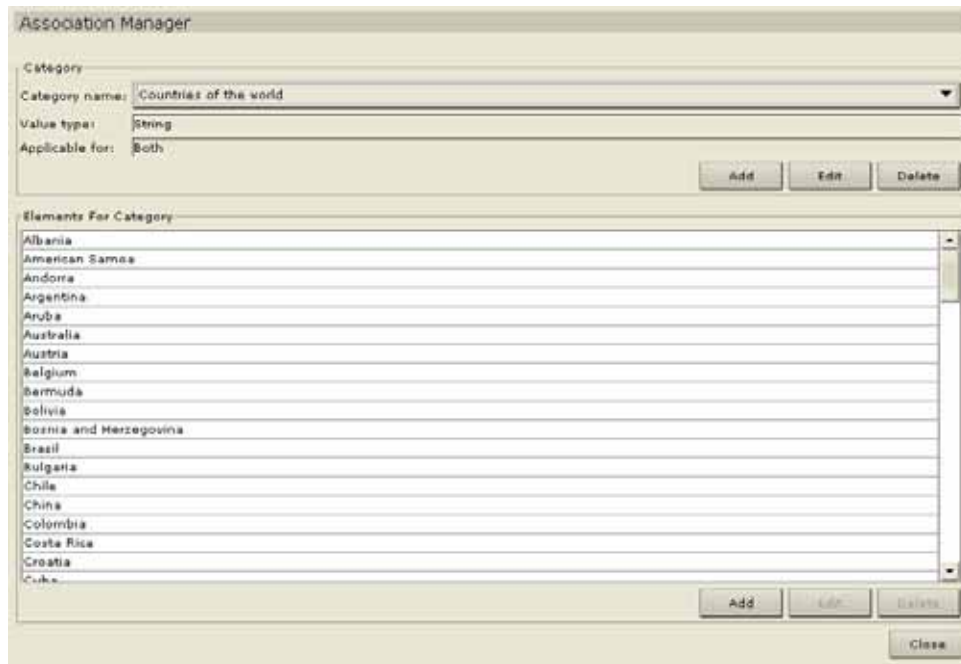


Figure 40 Association Manager Screen

2. Click **Add** in the **Element for Category** panel to add a new element. The **Add Element** window appears.

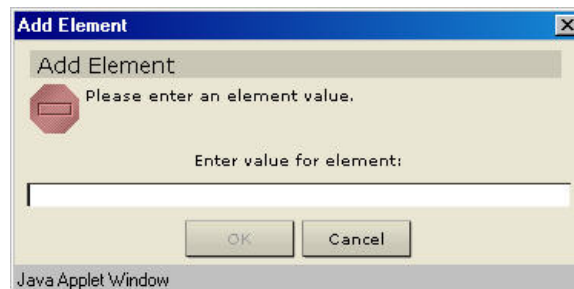


Figure 41 Add Element Window

3. Type the new element name in the **Enter Value for Element** field.
4. Click **OK** to add the element or **Cancel** to exit the window. The new element appears in the **Elements For Category** panel.
5. Click **Close** to close the **Association Manager** screen.
6. Repeat steps 1 through 5 to add other elements.

Edit Element

1. On the **Associations** menu, click **Association Manager**. The **Association Manager** screen appears.
2. Select the element to be edited from the **Element For Category** list and click **Edit** in the **Elements For Category** panel. The **Edit Element** window appears.

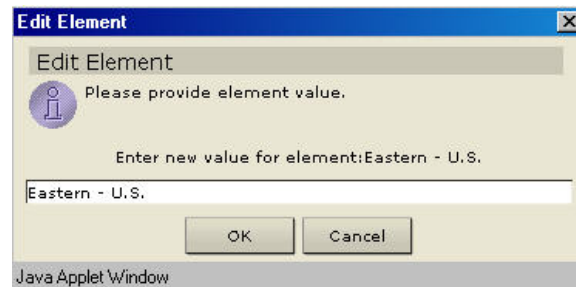


Figure 42 Edit Element Window

3. Type the new name of the element in the **Enter New Value for Element** field.
4. Click **OK** to update the element or **Cancel** to close the window. The new element name is displayed in the **Element For Category** list.
5. Click **Close** to close the **Association Manager** screen.
6. Repeat steps 1 through 5 to edit other elements.

Delete Element

Deleting an element removes that element from all Port associations, leaving association fields blank.

1. On the **Associations** menu, click **Association Manager**. The **Association Manager** screen appears.
2. Select the element to be deleted from the **Element For Category** list and click **Delete** in the **Elements For Category** panel. The **Delete Element** window appears.

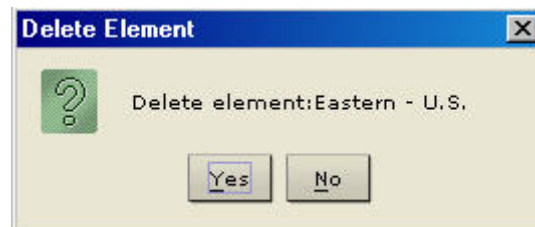


Figure 43 Delete Element Window

3. Click **Yes** to delete the element or **No** to close the window. The element name disappears from the **Element For Category** list.
4. Click **Close** to close the **Association Manager** screen.
5. Repeat steps 1 through 4 to delete other elements.

Note: Deleting an element removes the element from all device and port category associations, leaving all pre-associated element fields blank.

Association Wizard

The Association Wizard guides you through steps to create *categories* and their associated *elements*, as described in the **Association Manager** section above, then automates the creation of related **Port Groups** and **Policies** for those elements.

1. On the **Associations** menu, click **Association Wizard**. The Association Wizard screen appears.



Figure 44 Association Wizard Overview

2. After reading the overview, click **Next**. The **Category and Elements** screen of the Wizard appears.

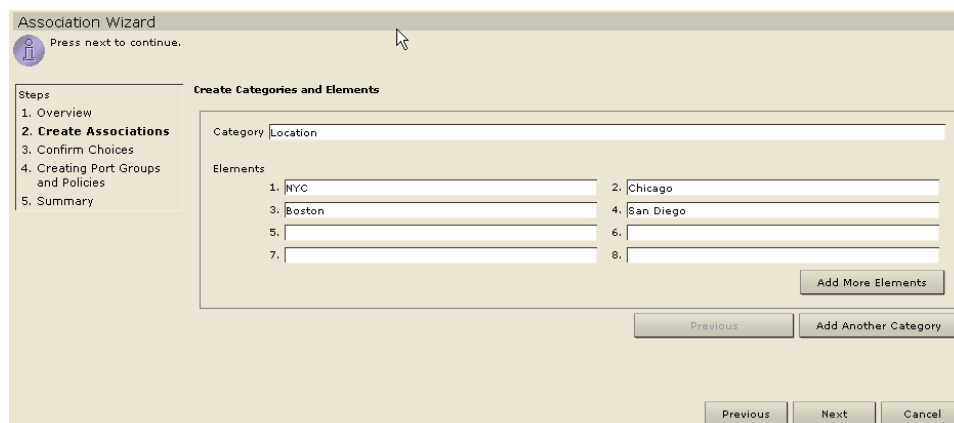


Figure 45 Association Wizard - Category And Elements Screen

3. Type the name of a category you wish to organize your ports by (for example: *Location*) in the **Category** field. Maximum length is 31 characters.
4. Type a unique name of each element in that category in the **Elements** fields below. Maximum length is 19 characters. These elements are used to group your ports within the category (for example: *LA Market Area*, *Chicago Market Area*, etc.). If you require more elements for this category, click **Add More Elements**.

5. If you wish to create another category, click **Add Another Category** and repeat steps 3 and 4.

Association Wizard
Press next to continue.

Steps

1. Overview
- 2. Create Associations**
3. Confirm Choices
4. Creating Port Groups and Policies
5. Summary

Create Categories and Elements

Category:

Elements:

1. Sales	2. Monitoring
3. Production	4. Testing Rack
5. Demo Rack	6.
7.	8.

Figure 46 Adding Another Category

6. When you are done creating categories, click **Next** at the bottom of the screen. The **Confirm Choices** screen of the Wizard appears.

Association Wizard

Steps

1. Overview
2. Create Associations
- 3. Confirm Choices**
4. Creating Port Groups and Policies
5. Summary

Confirm Choices

The following categories and elements will be created:

Category	Elements
Function	Sales, Monitoring, Production, Testing Rack, Demo Rack

Figure 47 Association Wizard - Confirm Choices

7. Review the list of categories and associated elements that will be created. Click **Previous** if you need to go back and make changes. If everything is correct, click **Finish**.

8. CC-SG will show a progress bar while it is creating the associations, port groups and policies. When this is complete, the **Association Wizard Summary** screen appears displaying the list what was created. Click **Done** to exit the wizard.

Association Wizard			
Steps 1. Overview 2. Create Associations 3. Confirm Choices 4. Creating Port Groups and Policies 5. Summary	Summary		
	The following Port groups have been created with their corresponding policies:		
	Category: Location		
	Elements	Groups	Policies
	LA Market Area	LA Market Area Ports	Allow LA Market Area Ports
	Chicago Market Area	Chicago Market Area Ports	Allow Chicago Market Area Ports
	New York Market Area	New York Market Area Ports	Allow New York Market Area Ports
	Atlanta Market Area	Atlanta Market Area Ports	Allow Atlanta Market Area Ports
	Category: Function		
	Elements	Groups	Policies
	Sales Servers	Sales Servers Ports	Allow Sales Servers Ports
	Monitoring	Monitoring Ports	Allow Monitoring Ports
	Production	Production Ports	Allow Production Ports
	Testing Rack	Testing Rack Ports	Allow Testing Rack Ports
	Demo Rack	Demo Rack Ports	Allow Demo Rack Ports

Figure 48 Association Wizard - Summary Screen

9. The Association Wizard has now created a port group for each element, and a policy for each port group. If the element names were not unique, the default port groups and policies cannot be created—see **Appendix F: Troubleshooting** for additional information. You can now add ports to these port groups using the **Port Group Manager**. To make changes to any of the categories, from the **Associations** menu, click **Association Manager**. To make changes to any of the policies, from the **Associations** menu, click **Policy Manager**. By default, the Association Wizard sets the policy for control access at all times.

Import Categories, Devices, Ports from CSV File

To expedite configuration, you can import pre-defined categories, elements of those categories, and the ports and devices to which the categories apply from a CSV file. After importing, you can have CC-SG validate the file to ensure the file was formatted properly. If errors are discovered, they are displayed.

Once successfully imported, the categories and elements are added to the CC-SG database and they are applied to the ports and devices as specified in the file. The devices specified in the CSV file must have been added to CC-SG prior to importing—please see **Add Device** in **Chapter 5: Adding Devices and Device Groups**. Also, the ports specified in the CSV file must have been configured in CC-SG prior to importing—please see **Configure Port** in **Chapter 6: Configuring Ports and Port Groups**.

On the **Setup** menu, click **Scripts**, then **Import Categories**. The **Import Categories** screen appears.

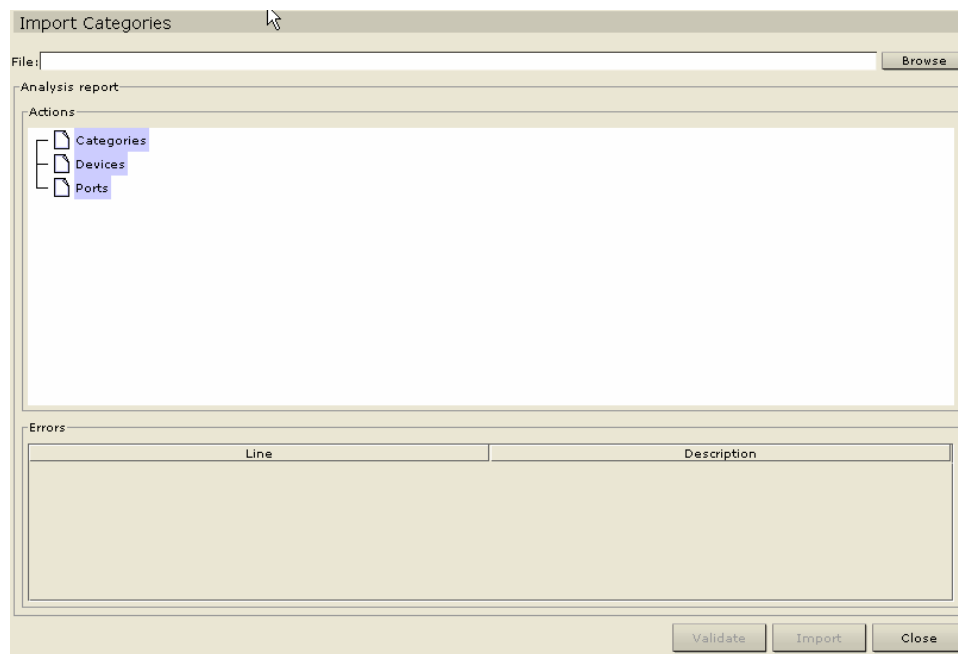


Figure 49 Import Categories Screen

1. Click **Browse** and select a CSV file.
2. Click **Validate** to ensure it is in the correct format. If there are errors, they will be displayed so they can be corrected and you can re-import the file.
3. If no errors are found or after correcting any errors, click **Import** to import the file.

CSV File Format

The entries in the CSV file are case-sensitive and each row in the CSV file has this format:
 {tag},{value}[, {value}, ...]

TAG	SUBSEQUENT FIELDS	COMMENTS
CATEGORY	Category Name,ValueType,Applicability	Value Type is String or Integer; Applicability is Device, Port, Both
CATEGORYELEMENT	Category Name, Element Name	For each element in category
DEVICE	Device Name, Category Name, Element Name	For each device and for each category that applies to it.
PORT	Device Name, Raritan Port ID or Port Number, Port Name, Category Name, Element Name	For each port and for each category that applies to it. For iLO/RILOE, PowerStrip, and IPMI device, the port number will be used; for all other devices, the Raritan Port ID will be used.

CSV File Example

```

CATEGORY,Memory,String,Port
CATEGORYELEMENT,Memory,256 MB
CATEGORYELEMENT,Memory,512 MB
CATEGORYELEMENT,Memory,1024 MB
CATEGORY,OS,String,Port
CATEGORYELEMENT,OS,UNIX
CATEGORYELEMENT,OS,WINDOWS
CATEGORYELEMENT,OS,LINUX
CATEGORY,Location,String,Device
CATEGORYELEMENT,Location,Aisle 1
CATEGORYELEMENT,Location,Aisle 2
CATEGORYELEMENT,Location,Aisle 3
DEVICE,192.168.32.20, Location,Aisle 2
PORT,192.168.32.20, Raritan Port ID, Port 3, OS,UNIX
PORT,192.168.32.20, Raritan Port ID, Port 3, Memory,1024 MB
  
```

Once successfully imported, you should see something like:

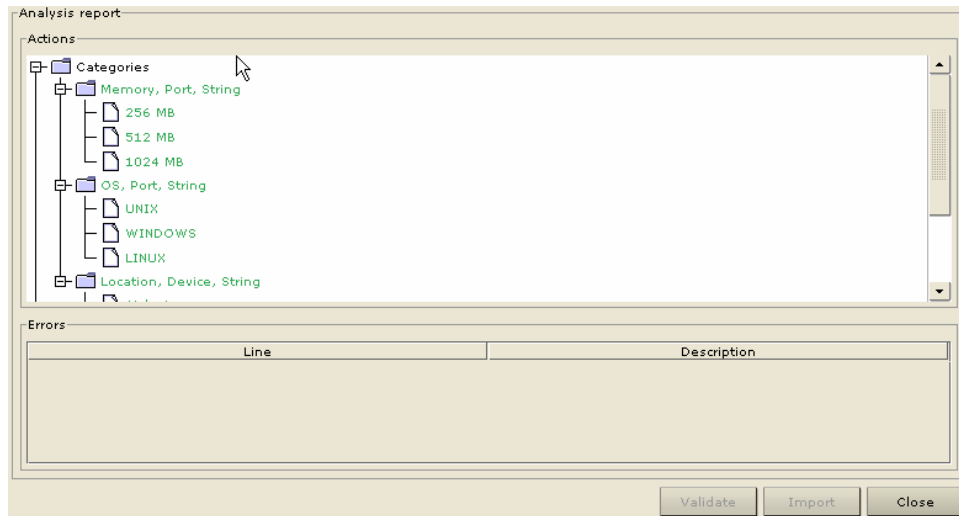


Figure 50 Analysis Report Screen

If necessary, refer to **Appendix F: Troubleshooting** for problem resolution.

Chapter 5: Adding Devices and Device Groups

Device Manager

Device Manager commands allow you to configure Dominion series and IP-Reach units and their individual ports. From a CC-SG perspective, connection to a remote target device is made via a serial or KVM port. You can configure the system on a port-by-port basis in order to easily access remote target devices.

When you click on the **Devices** tab and select a device from the Devices tree, the View Device screen will automatically appear, displaying information about the selected device. For easier identification, KVM, Serial, and Power devices have different icons in the Devices tree. In addition, availability status of each device also has a different icon. For a description of what the icons represent, please see the table below.

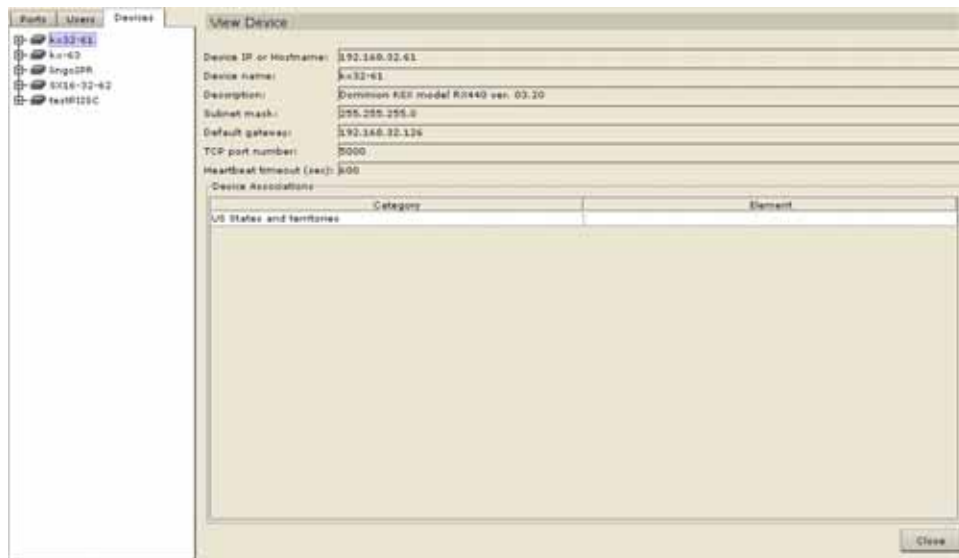


Figure 51 The Devices Tab And View Devices Screen

Device Icons

ICON	MEANING
	Device available
	Port available
	KVM port connected – in current user session
	Port paused – because device is paused
	Port unavailable – because device is unavailable
	Port busy – other user connected to port
	Serial port available – not connected
	Serial port connected – in current user session
	Serial port busy – other user connected to port
	Serial port unavailable – device is down and unavailable
	Serial port paused – because device is paused
	Device paused
	Device unavailable – device restarted and e = 33 is thrown
	Power strip available
	Outlet port available
	Power strip paused
	Outlet port paused

Important! Many of the menu bar commands can be accessed by right-clicking on a Device icon and selecting a command from the shortcut menu that appears.

Add Device

Use this command to add a new device to the system.

1. Click on the **Devices** tab.
2. On the **Devices** menu, click **Device Manager**, and then click **Add Device**. The **Add Device** selection screen appears.

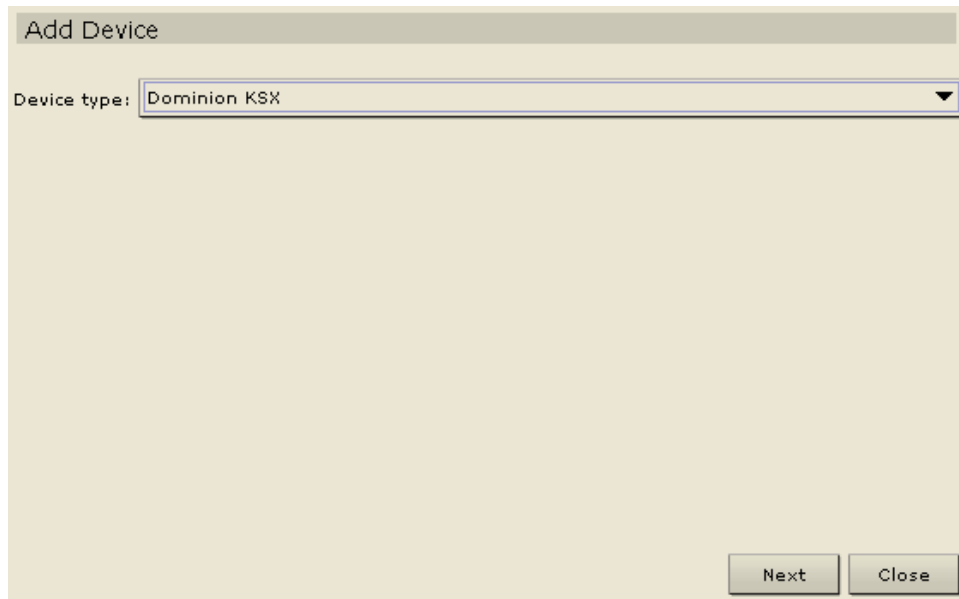


Figure 52 Add Device Selection Screen

3. Click on the **Device Type** drop-down arrow and select a type of device from the list.
4. Click **Next** to proceed. The **Add Device** description screen appears. Depending on the type of device you selected, you will see a device in the Dominion family (KSX, KX, KX101, or SX), an IP-Reach, a Paragon II System Controller, an Intelligent Platform Management Interface (IPMI) v1.5 device, a PowerStrip, a Generic device (for example, a hub, Windows server, or Cisco router) or an iLO/RILOE screen.

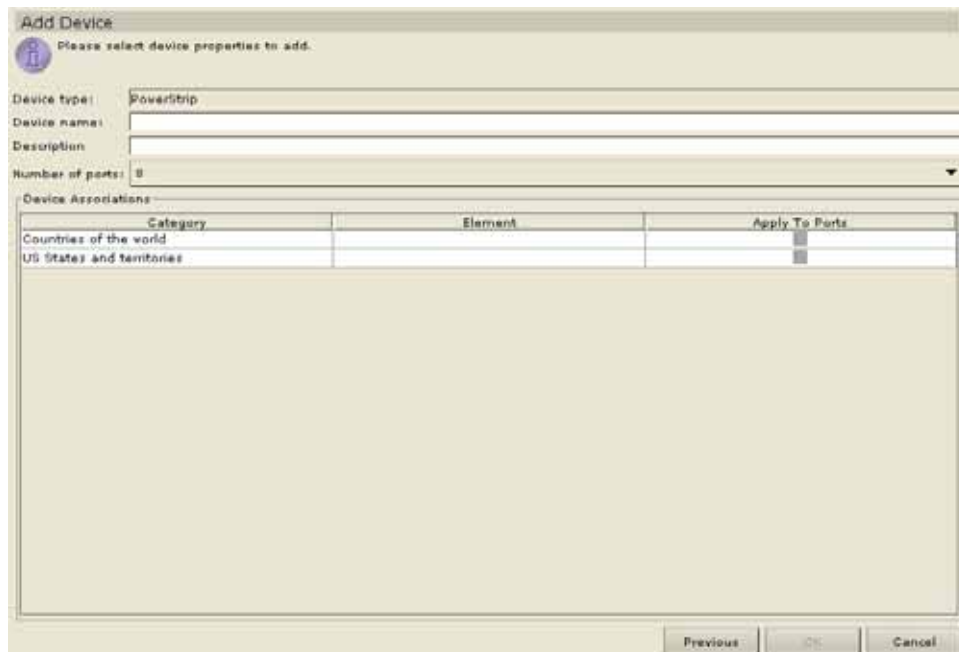
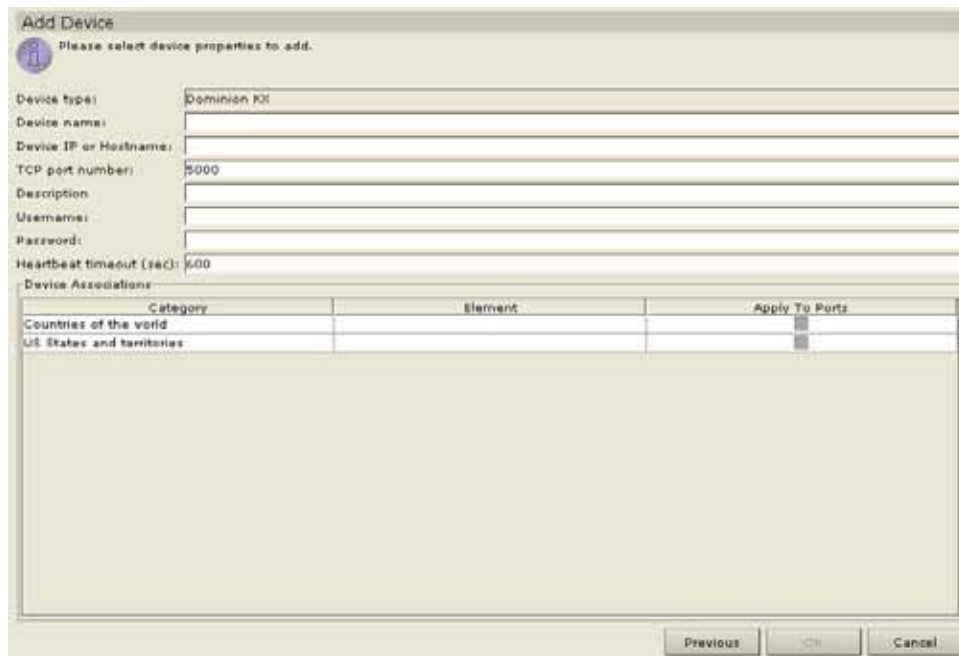


Figure 53 Add Device Screen for PowerStrip



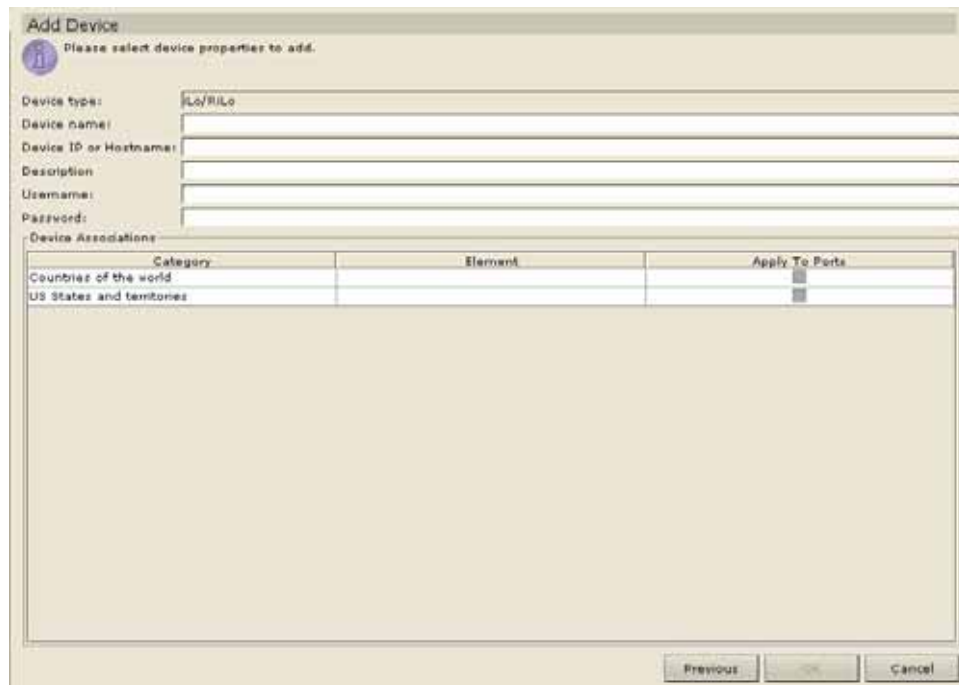
Add Device
Please select device properties to add.

Device type: Dominion KX
Device name:
Device ID or Hostname:
TCP port number: 5000
Description:
Username:
Password:
Heartbeat timeout (sec): 600

Device Associations

Category	Element	Apply To Ports
Countries of the world		☐
US States and territories		☐

Previous OK Cancel

Figure 54 Add Device Screen for Raritan Devices

Add Device
Please select device properties to add.

Device type: iLO/RILO
Device name:
Device ID or Hostname:
Description:
Username:
Password:

Device Associations

Category	Element	Apply To Ports
Countries of the world		☐
US States and territories		☐

Previous OK Cancel

Figure 55 Add Device Screen for iLO, RILOE

Add Device
Please select device properties to add.

Device type: IPMI Server

Device name:

Device IP or Hostname:

Description:

UDP Port: 623

Check interval: 600

Authentication: Password

Username:

Password:

Figure 56 Add Device Screen for IPMI Server (v 1.5)

Add Device
Please select device properties to add.

Device type: Generic Device

Device name:

Device IP or Hostname:

Description:

Device Associations

Category	Element	Apply To Ports
Region		☐
US States and territories		☐

Figure 57 Add Device Screen for Generic Device

5. Type the new device name in the **Device name** field.
6. Type the IP Address or Hostname of the new device in the **Device IP or Hostname** field. For hostname rules, see **Terminology/Acronyms** in **Chapter 1: Introduction**.
7. The TCP/UDP port number value will be populated automatically based on the device type. For example, the default UDP port for an IPMI device is **623**.
8. Type a description (or location) of the new device in the **Description** field.
9. Type the name used to log onto this device in the **Username** field.
10. Type the password needed to access this device in the **Password** field.
11. If applicable, type the time (in seconds) that should elapse before timeout between the new device and CC-SG in the **Heartbeat timeout (sec)** field.
12. For IPMI Servers, enter an **Interval** that is used to check for availability and an **Authentication Method**, which needs to match what has been configured on the IPMI Server.

Note: You will not see a TCP port number or Heartbeat timeout field for HP iLO/RILOE devices, older Dominion SX units (version 2.4 or earlier), IPMI Servers, and Generic devices.

13. Click **OK** to add the device or **Cancel** to exit without saving.
14. For Raritan devices, if the firmware version of the device is not compatible with CC-SG, a message will alert you and ask if you want to proceed (please see **Chapter 2: Accessing CC-SG** for additional information). Click **Yes** to add the device to CC-SG, or **No** to cancel the operation. You can easily upgrade the device firmware after adding it to CC-SG (see section **Upgrade Device** later in this chapter).
15. A **Device Created Successfully** message confirms that device has been added.
16. Repeat steps 1 through 12 to add other devices.

KX Devices with Encryption

CC-SG supports adding and managing Dominion KX devices, such as KX101, that have been configured with:

- SSL authentication and no data encryption
- SSL authentication and data encryption
- SSL authentication and SSL data encryption
- No authentication and no encryption

Refer to Raritan's **Dominion KX User Guide** for definitions of these encryption modes.

Edit Device

Use this command to rename a device and /or modify its properties.

1. Click on the **Devices** tab and select a device from Devices tree.
2. On the **Devices** menu, click **Device Manager**, and then click **Edit Device**. The **Edit Device** screen appears.

Edit Device

Please select device properties to add.

Device IP or Hostname: 192.168.51.223

Device type: Dominion KX

Device name: KX-223

Description:

Subnet mask: 255.255.255.0

Default gateway: 192.168.51.126

TCP port number: 5000

Heartbeat timeout (sec): 120

Device Association

Category	Element	Apply To Ports
Countries of the world		☐
US States and territories		☐

OK Cancel

Figure 58 Edit Device Screen

3. Type the new device properties in the appropriate fields on this screen, up to and including selecting different or new **Category** and **Element** properties from the **Device Association** panel.
4. Click **OK** to edit the device or **Cancel** to exit with modifying. A **Device Updated Successfully** message confirms that device has been modified.
5. Repeat steps 1 through 4 to edit other devices.

Delete Device

1. Click on the **Devices** tab and select a device from Devices tree.
2. On the **Devices** menu, click **Device Manager**, and then click **Delete Device**. The **Delete Device** screen appears.



Figure 59 Delete Device Screen

3. Click **OK** to delete the device or **Cancel** to exit without deleting. A **Device Deleted Successfully** message confirms that the device has been deleted.
4. Repeat steps 1 through 3 to delete other devices.

Bulk Copy

The Bulk Copy command allows you to copy the assigned categories and elements from one device to multiple other devices. Please note that categories and elements are the only properties copied in this process.

1. Click on the **Devices** tab and select a device from Devices tree.
2. On the **Devices** menu, click **Device Manager**, and then click **Bulk Copy**. The **Bulk Copy** screen appears.

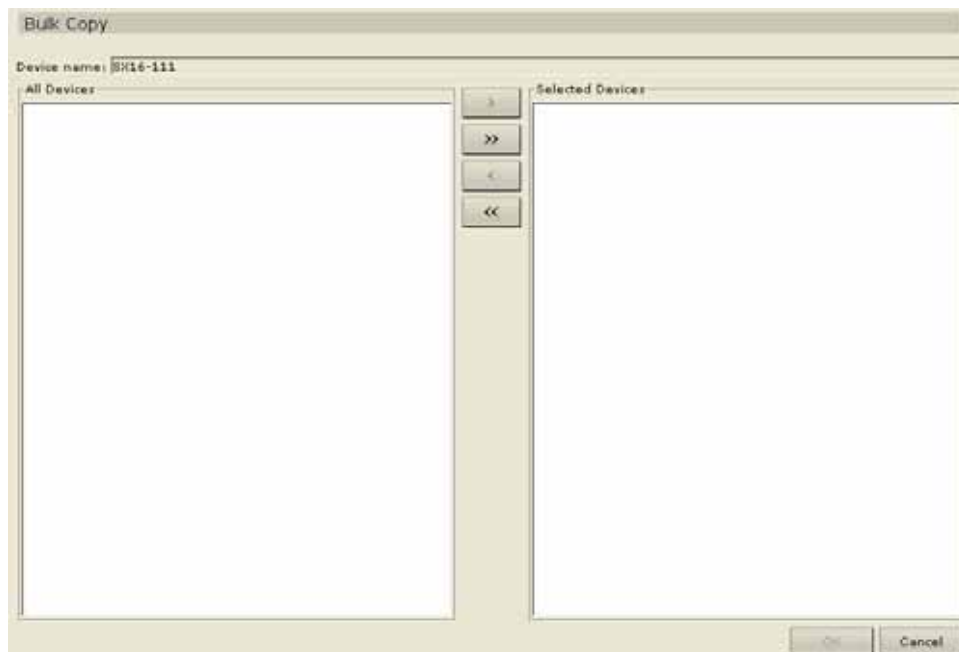


Figure 60 Bulk Copy Screen

3. In the **All Devices** list, select the device(s) to which you are copying the categories and elements of the device in the **Device Name** field.
4. Click **>** to add a device to the **Selected Devices** list.
5. To remove a device from the **Selected Devices** list, select the device, and click **<**.
6. Click **OK** to bulk copy or **Cancel** to exit without copying. A **Device Copied Successfully** message confirms that device categories and elements have been copied.
7. Repeat steps 1 through 6 to copy other categories and elements of other devices.

Backup Device Configuration

Use this command to back up all user configuration and system configuration files. If anything happens to your system, you can restore your previous configurations from memory.

Note: Only for Dominion SX 2.5 devices or later, network settings, such as IP address, subnet mask, IP gateway are not included in the backup file.

1. Click on the **Devices** tab and select a device from the Devices tree.
2. On the **Devices** menu, click **Device Manager**, and then click **Backup Device Configuration**. The **Backup Device Configuration** screen appears.



Figure 61 Backup Device Configuration Screen

3. Click **OK** to back up the device configuration or **Cancel** to exit without backing up. A **Device Configuration Backed Up Successfully** message confirms that device configuration has been backed up.
4. Repeat steps 1 through 3 to back up other device configurations.

Restore Device Configuration

This command allows you to restore a previously backed-up device configuration.

1. Click on the **Devices** tab and select a device from the Devices tree.
2. On the **Devices** menu, click **Device Manager**, and then click **Restore Device Configuration**. The **Restore Device Configuration** screen appears.

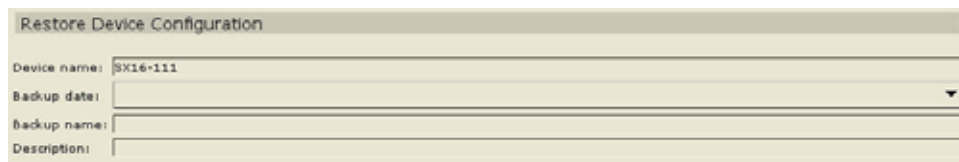


Figure 62 Restore Device Configuration Screen

3. Click on the **Backup Date** drop-down arrow and select a date from the list of when you last made a back up of the device.
4. Click **OK** to restore the back up or **Cancel** to exit without restoring.
5. When the Restart message appears, click **Yes** to restart the device or **No** to close the window without restarting. A **Device Configuration Restored Successfully** message confirms that all user and system configuration data has been restored.
6. Repeat step 1 through 5 to restore other devices' configurations.

Copy Device Configuration

This command allows you to copy configurations from one device to another or multiple devices.

Note: Configuration can only be copied between Dominion SX units and DSX units that have the same number of ports.

1. Click on the **Devices** tab and select the device whose configuration you wish to copy to other devices from the Devices tree.
2. On the **Devices** menu, click **Device Manager**, and then click **Copy Device Configuration**. The **Copy Device Configuration** screen appears.

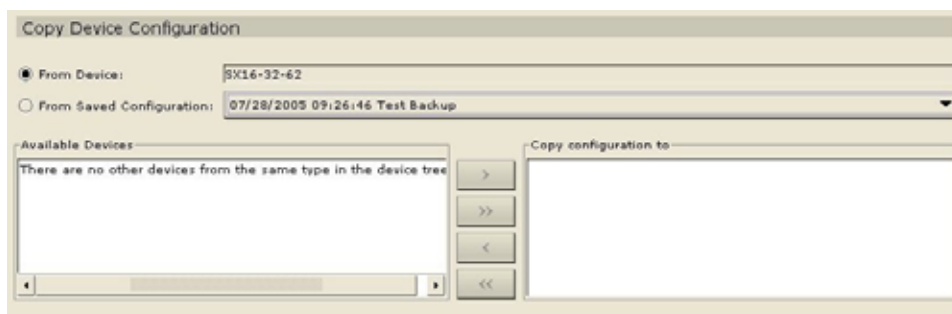


Figure 63 Copy Device Configuration Screen

3. If you have used the **Backup Device** option on this device, you can copy that configuration instead by selecting **From Saved Configuration** and then selecting the configuration from the saved configuration drop-down arrow.
4. Highlight the devices you want to copy this configuration to in the **Available Devices** column and click the right arrow to move them to the **Copy Configuration To** column. The left arrow moves selected devices out of the **Copy Configuration To** column.
5. Click **OK** to copy the configuration to the devices in the **Copy Configuration To** column, or **Cancel** to exit without copying. A **Restart** message appears after copying.
6. Click **Yes** to restart the device or **No** to close the window without restarting. A **Device Configuration Copied Successfully to** message confirms that device configuration has been copied.
7. Repeat steps 1 through 6 to copy other devices' configurations.

Upgrade Device

Use the Upgrade Device command to download new versions of device firmware.

1. Click on the **Devices** tab and select a device from the Devices tree.
2. On the **Devices** menu, click **Device Manager**, and then click **Upgrade Device**. The **Upgrade Device** screen appears.

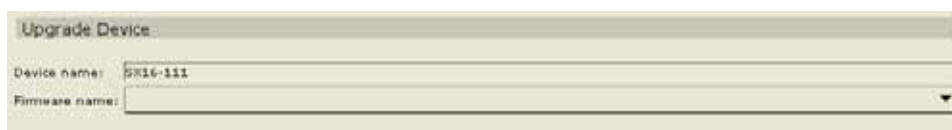


Figure 64 Upgrade Device Screen

3. Click on the **Firmware Name** drop-down arrow and select the appropriate firmware from the list (Raritan or your reseller will provide this information).
4. Click **OK** to upgrade the device or **Cancel** to close the **Upgrade Device** screen.

If the firmware version of the device is not compatible with CC-SG, a message will alert you and ask if you want to proceed (please see **Chapter 2: Accessing CC-SG** for additional information). Click **Yes** to upgrade the device, or **No** to cancel the operation.

5. A **Restart** message appears; click **Yes** to restart the device or **No** to close the window without restarting.
6. A **Device Upgraded Successfully** message confirms that the device has been upgraded.
7. Repeat steps 1 through 6 to upgrade other devices.

Note: Firmware for iLO/RILOE cannot be upgraded using CC-SG.

Ping Device

You can ping a device to determine if the device is available in your network.

1. Click on the **Devices** tab and select a device from the Devices tree.
2. On the **Devices** menu, click **Device Manager**, and then click **Ping Device**. The **Ping Device** screen appears, showing the result of the ping.



Figure 65 Ping Device Screen

3. Click **Close** to clear this screen.
4. Repeat steps 1 through 3 to ping other devices.

Restart Device

Use the Restart Device command to restart a device.

1. Click on the **Devices** tab and select a device from the Devices tree.
2. On the **Devices** menu, click **Device Manager**, and then click **Restart Device**. The **Restart Device** screen appears.

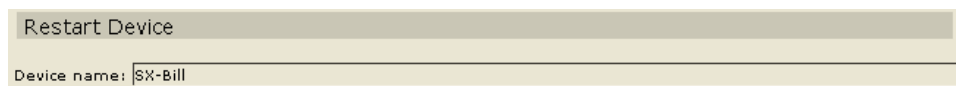


Figure 66 Restart Device Screen

3. Click **OK** to restart the device or **Cancel** to exit without restarting. A **Device Restart Successfully** message confirms that the device has been restarted.
4. Repeat steps 1 through 3 to restart other devices.

Pause Device

You can pause a device to temporarily suspend CC-SG's control of it without losing any of the configuration data stored within the CC-SG Server.

1. Click on the **Devices** tab and select a device from the Devices tree.
2. On the **Devices** menu, click **Device Manager**, and then click **Pause Management**. The indicator of the device being paused is its icon changing from a grey 'active' state to a red 'paused' state in the Devices tree.

Resume Device

After pausing a device, have it continue with its normal activity by commanding it to resume.

1. Click on the **Devices** tab and select the paused device from the Devices tree.
2. On the **Devices** menu, click **Device Manager**, and then click **Resume Management**. The device icon changes from the red 'paused' state to a grey 'active' state.

View Devices

Regular View

Select this command to view devices in the Devices tree grouped in default view (you can change the regular view by assigning new criteria in custom view, see the next section **Custom View**).

1. Click on the **Devices** tab.
2. On the **Devices** menu, click **Change View**, and then click **Regular View**. The **Regular View** of the Devices tree appears.

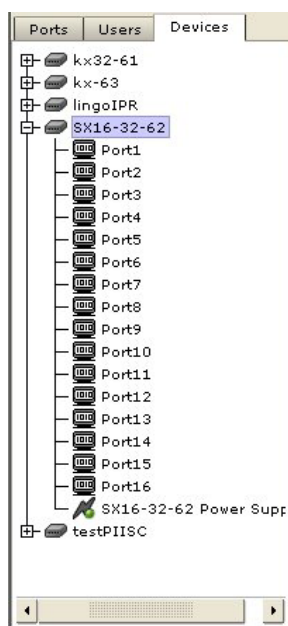


Figure 67 Devices Tree Regular View Screen

Known ports are nested under their parent devices. Right-click on the tree, then click **Port Sorting Options**, then **Sort By Port Name** or **Sort By Port Status** to arrange the ports within their devices alphabetically by name or by availability status. Ports arranged by status are sorted alphabetically within their connection status grouping. Devices will also be sorted accordingly.

Custom View

You can customize the Devices tree by organizing devices to appear in a particular format. You might want to view devices by Country, by Time Zone, or by any other option that helps you differentiate between them. Set up a Custom View using the next few sessions. Please also see section **Association Manager** in **Chapter 4: Creating Associations** for more details on adding Categories to CC-SG.

1. Click on the **Devices** tab.
2. On the **Devices** menu, click **Change View**, and then click **Custom View**. The **Custom View** screen appears.

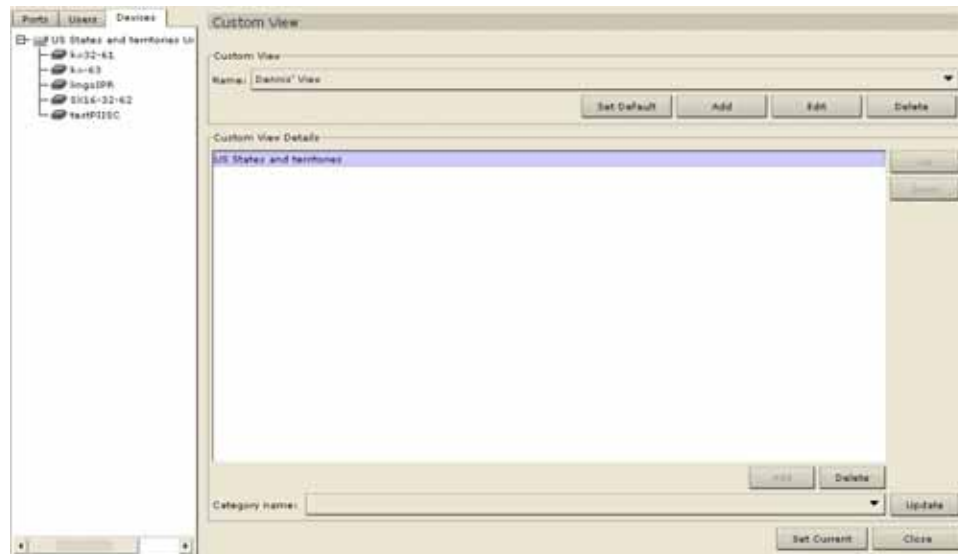


Figure 68 Custom View Screen

3. To customize your view, click on the **Name** drop-down arrow and select a custom view that has already been saved in the database. Details of the View categories appear in the **Custom View Details** field.
4. Click **Set Current** to arrange the Devices tree to reflect the selected custom view.
5. Click **Set Default** if you want the selected custom view to be displayed when logging into CC-SG.
6. Click **Close** to close the **Custom View** screen.
7. Repeat steps 1 through 5 to change custom view.

Known ports are nested under their parent devices. Right-click on the tree, then click **Port Sorting Options**, then **Sort By Port Name** or **Sort By Port Status** to arrange the ports within their devices alphabetically by name or by availability status. Ports arranged by status are sorted alphabetically within their connection status grouping. Devices will also be sorted accordingly.

Add Custom View

1. Click on the **Devices** tab.
2. On the **Devices** menu, click **Change View**, and then click **Custom View**. The **Custom View** screen appears.
3. In the **Custom View** panel, click **Add**. An **Add Custom View** window appears.



Figure 69 Add Custom View Window

4. Type a new custom view name and click **OK** or click **Cancel** to close the window. The new view name appears in the **Name** field.
5. In the **Custom View Details** panel, click on the drop-down arrow at the bottom of the panel. This list contains categories that you can use to filter custom views. Select a detail from the drop-down list and click **Add** to add the detail to the **Custom View Details** panel. Select as many details as needed.
6. To re-order the details in the **Custom User Details** panel, select a detail and use the **Up** and **Down** buttons to arrange details in the order you want devices sorted. To remove a detail from the list, select the detail and click the **Delete** button in the **Custom User Details** panel.
7. Click **Update** to update the custom view. A **Custom View Updated Successfully** message confirms that the custom view has been updated.
8. Click **Set Current** to arrange the Devices tree to reflect the selected custom view.
9. Click **Close** to close the **Custom View** screen.
10. Repeat steps 1 through 9 to add a new custom view.

Edit Custom View

1. Click on the **Devices** tab.
2. On the **Devices** menu click **Change View**, and then click **Custom View**. The **Custom View** screen appears.
3. Click on the **Name** drop-down arrow in the **Custom View** panel and select the custom view to be edited. Click **Edit**. An **Edit Custom View** window appears.

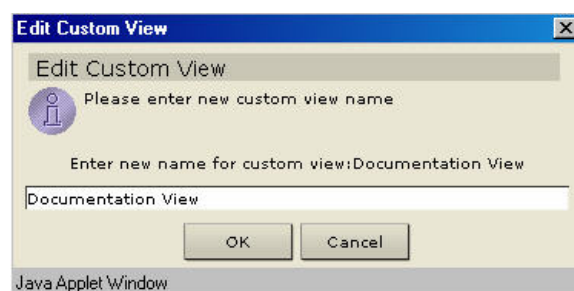


Figure 70 Edit Custom View Window

4. Type a new custom view name and click **OK** to confirm or **Cancel** to close window.

5. In the **Custom View Details** panel, click on the drop-down arrow at the bottom of the panel. This list contains categories that you can use to filter custom views. Select a detail from the drop-down list and click **Add** to add the detail to the **Custom View Details** panel. Select as many details as needed.
6. To re-order the details in the **Custom User Details** panel, select a detail and use the **Up** and **Down** buttons to arrange details in the order you want devices sorted. To remove a detail from the list, select the detail and click the **Delete** button in the **Custom User Details** panel.
7. Click **Update** to update custom view. A **Custom View Updated Successfully** message confirms that the custom view has been updated.
8. Click **Set Current** to arrange the Devices tree to reflect the selected custom view.
9. Click **Close** to close the **Custom View** screen.
10. Repeat steps 1 through 9 to edit other custom views.

Delete Custom View

1. Click on the **Devices** Tab.
2. On the **Devices** menu click **Change View**, and then click **Custom View**. The **Custom View** screen appears.

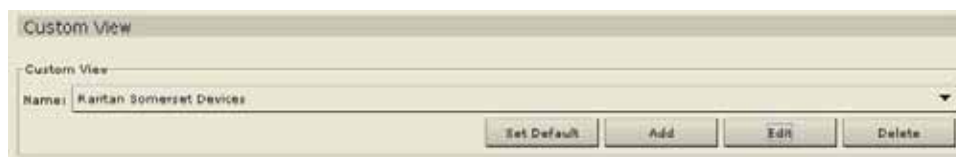


Figure 71 Custom View Screen

3. Click on the **Name** drop-down arrow in the **Custom View** panel and select the custom view to be deleted.
4. Click on the **Delete** button in the **Custom View** panel. A **Delete Custom View** window appears.

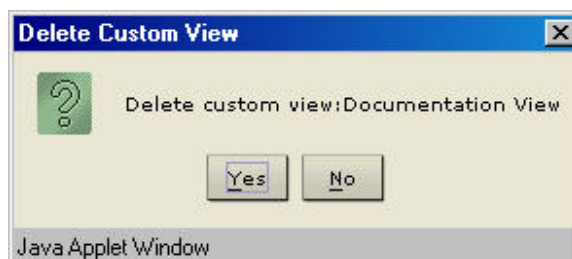


Figure 72 Delete Custom View Window

5. Click **Yes** to delete the custom view or **No** to close the window.
6. Click **Close** to close the **Custom View** screen.
7. Repeat steps 1 through 6 to delete other custom views.

Topological View

Use the Topological View command to view the structural setup of all the connected appliances in your configuration.

1. Click on the **Devices** tab and select a device from the Devices tree.
2. On the **Devices** menu, click **Topological View**. The **Topological View** for the selected device appears.



Figure 73 Topological View Screen

3. Navigate through the Topological View in the same way you navigate through the Devices tree; click on the + or – to expand or collapse the view.
4. Click **Close** to close **Topological View** screen.

Special Access to Paragon II System Devices

Paragon II System Controller (P2-SC)

Paragon II System Integration users can add their P2-SC devices to the CC-SG Devices tree and configure them via the P2-SC Admin application from within CC-SG. For more detailed directions on using P2-SC Admin, please see Raritan's **Paragon II System Controller User Guide**.

After adding your Paragon System device (the Paragon System includes the P2-SC device, connected UMT units, and connected IP-Reach units) to CC-SG, it will appear in the Devices tree. Right-click on the Paragon System icon in the Devices tree and select **Launch Admin** to launch the Paragon II System Controller application in a new browser window and configure your PII UMT units.

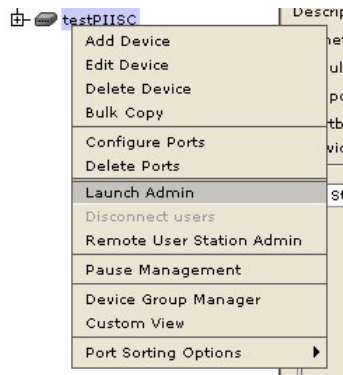


Figure 74 Paragon System Launch Admin Menu Option

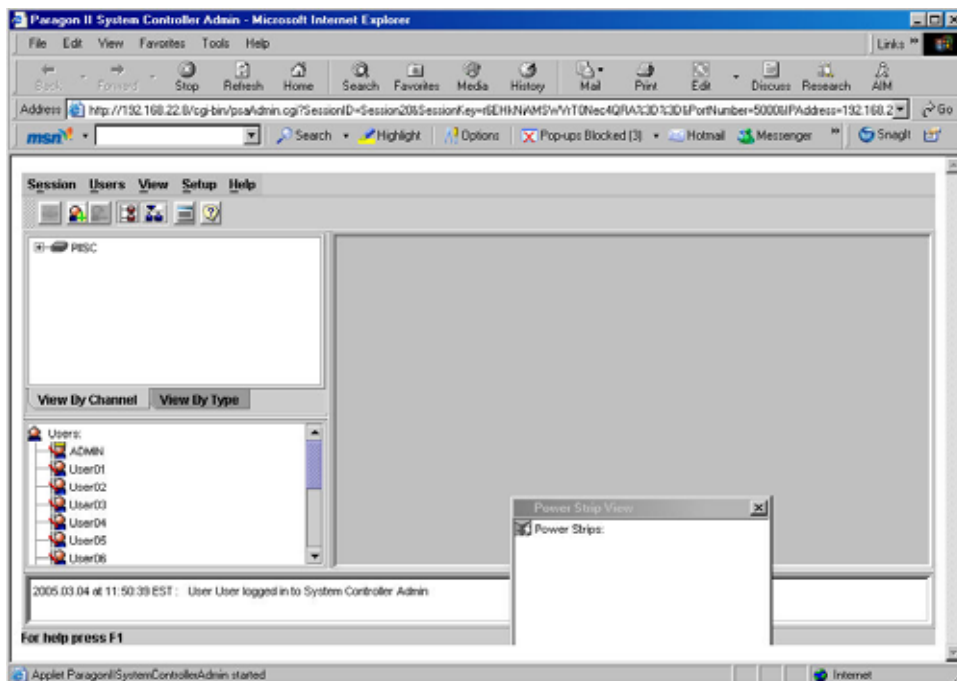


Figure 75 Paragon Manager Application Window

IP-Reach and UST-IP Administration

You can also perform administrative diagnostics on IP-Reach and UST-IP devices connected to your Paragon System setup directly from the CC-SG interface.

After adding the Paragon System device to CC-SG, it appears in the Devices tree. Right-click on the device icon in the Devices tree and select **Remote User Station Admin**. The Remote User Station Admin screen appears, listing all connected IP-Reach and UST-IP units. Click the **Launch Admin** button in the row of the device you want to work with to activate Raritan Remote Console and launch the blue device configuration screen in a new window.

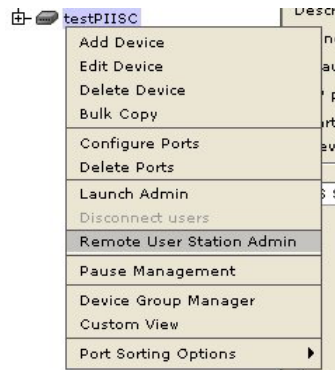


Figure 76 Remote User Station Admin Option

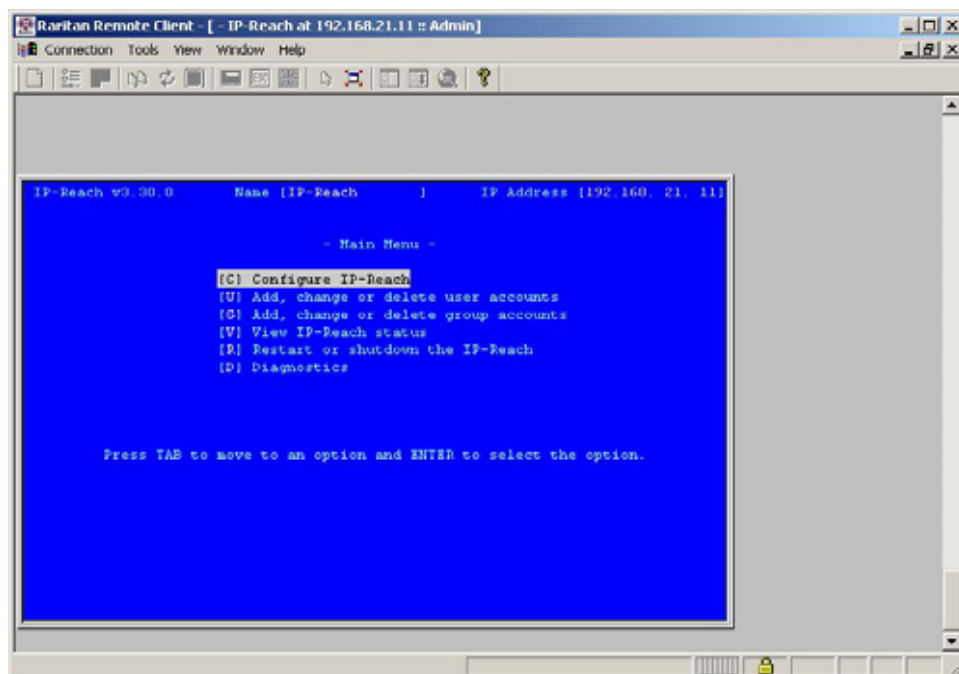


Figure 77 IP-Reach Administration Screen

Device Power Manager

Before using the Device Power Manager view, make a physical connection of a PowerStrip to a Dominion SX or Dominion KSX unit. When you add the PowerStrip device, define this connection in CC-SG. Once the PowerStrip is added, you can associate it with the Dominion SX serial ports or with Dominion KSX dedicated power ports. The Device Power Manager view displays outlets connected to devices' ports and allows you to remotely power on or power off associated ports, as well as monitor power, voltage, current, and temperature of the device.

1. In the **Devices** tree, select a device, then on the **Devices** menu, click **Device Power Manager**. The **Device Power Manager** screen appears.

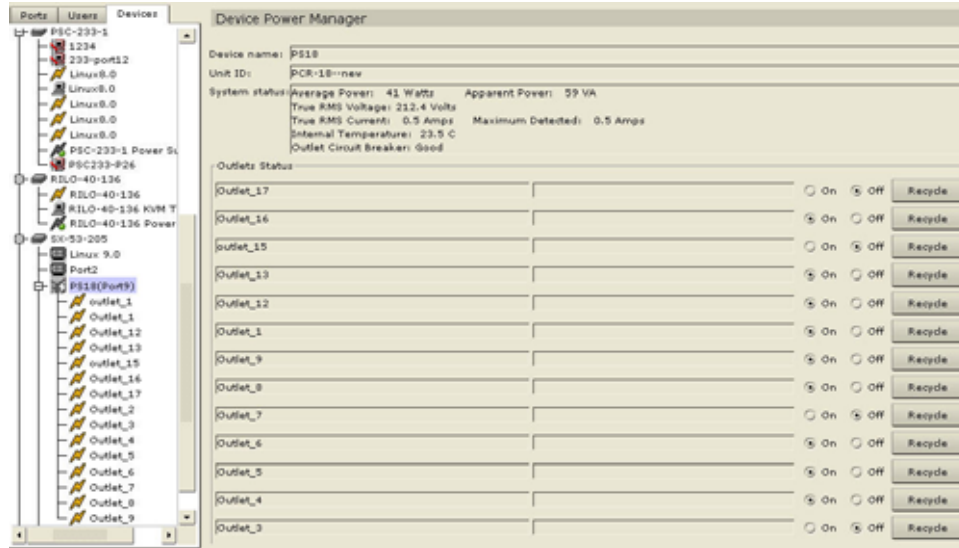


Figure 78 Device Power Manager Screen

2. The outlets will be listed in the **Outlets Status** panel. You may have to scroll to view all outlets.
3. Click the **On** or **Off** radio buttons for each outlet to power ON or power OFF the outlet.
4. Click **Recycle** to restart the device connected to the outlet.
5. Click **Close** to close the Device Power Manager screen.
6. Repeat steps 1 through 5 to monitor and control other devices.

Note: CC-SG automatically recognizes the outlets of PowerStrips attached to Dominion KX and P2-SC devices as additional ports of those devices; no PowerStrip association is necessary. These outlets are added and configured the same as any other device port. See section **Port Manager** in **Chapter 6: Configuring Ports and Port Groups** for instructions on adding and editing ports.

Discover Devices

Use this command to initiate a search for all devices on your system. The search will automatically detect all newly attached, and previously existing Raritan devices on your network, including Paragon, P2-SC, IP-Reach, Dominion KX, Dominion KSX units, IPMI servers, and CC-SGs. After locating the devices, you may connect them to your CC-SG system if they are not already connected.

Note: iLO/RILOE devices and Generic devices, such as hubs, Windows servers, Cisco routers, cannot be discovered. They have to be manually added.

1. Click on the **Devices** tab.
2. On the **Devices** menu, click **Discover Devices**. The Discover Devices screen appears.

Figure 79 Discover Devices Screen

3. Type the range of IP addresses where you expect to find the devices in the **From Address** and **To Address** fields. The **To Address** should be larger than the **From Address**. Specify a mask to apply to the range. If a mask is not specified, then a broadcast address of 255.255.255.255 is sent, which broadcasts to all local networks. To discover devices across subnets, you must specify a mask.
4. Click **Broadcast discovery** if searching for devices on the same subnet on which CC-SG resides. Uncheck **Broadcast discovery** to discover devices across all subnets.
5. To search for a particular type of device, highlight it in the list of Device types. By default, ALL device types are highlighted. Use **Ctrl+click** to select one or more device types.
6. Click **OK** to start the search, or **Cancel** to exit without searching, or **Stop** to discontinue the discovery process. Discovered devices appear in a **Discover Devices** list.

IP Address	Type	Name	Status	Description
192.168.51.124	CommandCenter Secure ...		Known	CommandCenter Secure ...
192.168.51.22	IPMI Server		Known	IPMI Server ver. 1.5
192.168.51.201	CommandCenter Secure ...		Unknown	CommandCenter Secure ...
192.168.51.74	CommandCenter Secure ...		Unknown	CommandCenter Secure ...
192.168.51.223	Dominion KSX	KSX223-1	Known	Dominion KSX model RK...
192.168.51.224	Dominion KX	KX224	Known	Dominion KX model DKX ...
192.168.51.229	Dominion SX	SX-229	Known	Dominion SX model SX1...
192.168.51.112	Dominion KSX	billskx	Known	Dominion KSX model RK...
192.168.51.184	Dominion KX	GMBDoNotUSE	Unknown	Dominion KX model DKX ...
192.168.51.187	Dominion KX	astdkx116-VER13	Unknown	Dominion KX model DKX ...
192.168.51.172	Dominion KX101	KX101-172	Unknown	KX101 model KX_KIM ver...
192.168.51.202	Dominion KX	Dominion-KX203	Unknown	Dominion KX model DKX ...
192.168.51.121	Dominion KX	billskx121	Unknown	Dominion KX model DKX ...
192.168.51.213	Dominion KX	ASTDKX416-VER13	Unknown	Dominion KX model DKX ...
192.168.51.120	Dominion KX	billskx120	Unknown	Dominion KX model DKX ...
192.168.51.252	Dominion KX	KX252	Unknown	Dominion KX model DKX ...
192.168.51.239	Dominion KX101	KX_KIM-0004	Unknown	KX101 model KX_KIM ver...
192.168.51.195	Dominion KX101	GMBKX101-195	Unknown	KX101 model KX_KIM ver...
192.168.51.139	Dominion KX101	KX_KIM-0008	Unknown	KX101 model KX_KIM ver...
192.168.51.69	Dominion KX101	billskx101	Unknown	KX101 model KX_KIM ver...
192.168.51.70	Dominion KX101	kx101a	Unknown	KX101 model KX_KIM ver...

Figure 80 Discovered Devices List Window

7. Select a device from the list and click **Add** to add the device to CC-SG or click **Close** to exit without adding the device. If you clicked **Add**, the Add Device screen appears.

Add Device
Please select device properties to add.

Device type: Dominion KX101
 Device name: KX_KIM-0005
 Device IP or Hostname: 192.168.51.159
 TCP port number: 5000
 Description: KX101 model KX_KIM ver. 4.3
 Username:
 Password:
 Heartbeat timeout (sec): 600

Device Associations

Category	Element	Apply To Ports
Countries of the world		☐
US States and territories		☐

Previous OK Cancel

Figure 81 Add Device Screen

8. Type the user name and password (that were created specifically for CC-SG in the device) in the **Username** and **Password** fields to allow CC-SG to authenticate the device when communicating with it in the future. Select a **Category** or **Element** to apply to the device.
9. Click **OK** to add the new device or **Cancel** to exit without adding. To return to the previous screen, click **Previous**. A **Device Added Successfully** message confirms that the device has been added.
10. Click **Previous** to return to the **Discover Devices** screen and add another device from the list if so desired.
11. Repeat steps 1 through 10 to find and add other devices.

Device Group Manager

Use the Device Groups Manager screen to add, edit, assign, and remove device groups and the rules that govern them. First add a Device Group, then add a Device Rule(s) to make working with and viewing devices easier.

Add Device Group

1. On the **Associations** menu, click **Groups Manager**, and then click **Device Group Manager**. The Device Group Manager screen appears.

Figure 82 Device Groups Manager Screen

2. Click **Add** in the **Groups** panel. The Add Device Group window appears.

Figure 83 Add Device Group Window

3. Type a device group name in the **Enter Device Group Name** field. Click **OK** to add the group or **Cancel** to close the window. The new group name will appear in the **Group Name** field.
4. Click **Close** to close **Device Groups Manager** screen.
5. Repeat steps 1 through 4 to add other device groups.

Edit Device Group Name

1. On the **Associations** menu, click **Groups Manager**, and then click **Device Group Manager**. The Device Group Manager screen appears.

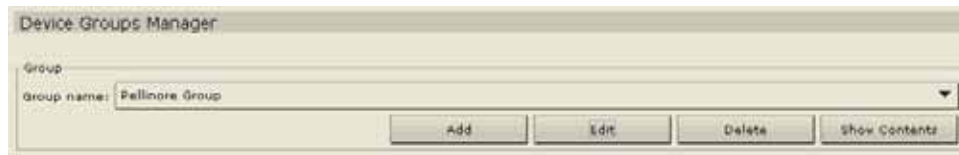


Figure 84 Device Groups Manager Screen

2. Click on the **Groups** drop-down arrow and select the group to be edited from the list. Click **Edit** and the Edit Device Group window appears.



Figure 85 Edit Device Group Window

3. Type the new name for the device group in the **Enter New Name for Device Group** field. Click **OK** to edit the device group or **Cancel** to close the window. The new name appears in the **Group Name** field.
4. Click **Close** to close **Device Groups Manager** screen.
5. Repeat steps 1 through 4 to edit other device group names.

Delete Device Group

1. On the **Associations** menu, click **Groups Manager**, and then click **Device Group Manager**. The Device Groups Manager screen appears.

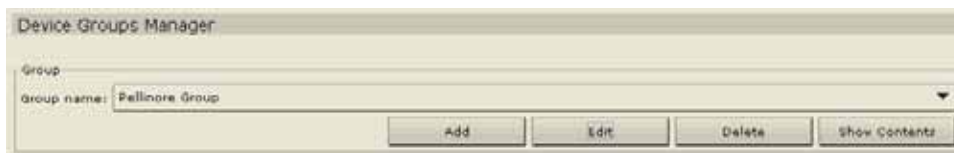


Figure 86 Device Groups Manager Screen

2. Click on the **Group Names** drop down arrow and select the device group to be deleted. Click **Delete** and the Delete Device Group window appears.

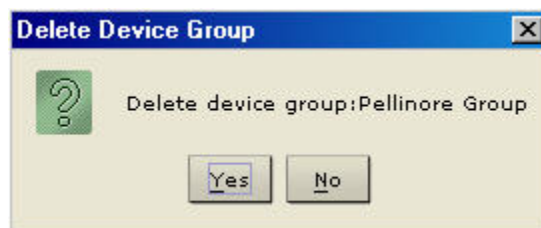


Figure 87 Delete Device Group Window

3. Click Yes to delete the group or **No** to **Cancel** and close the window.
4. Click **Close** to close **Device Groups Manager** screen.
5. Repeat steps 1 through 4 to delete other devices.

Add Device Rule

After adding a device group, apply one or more rules to the group so that devices can be grouped by matching parameters and you have a navigable Devices tree.

1. On the **Associations** menu, click **Groups Manager**, and then click **Device Group Manager**. The Device Groups Manager screen appears.

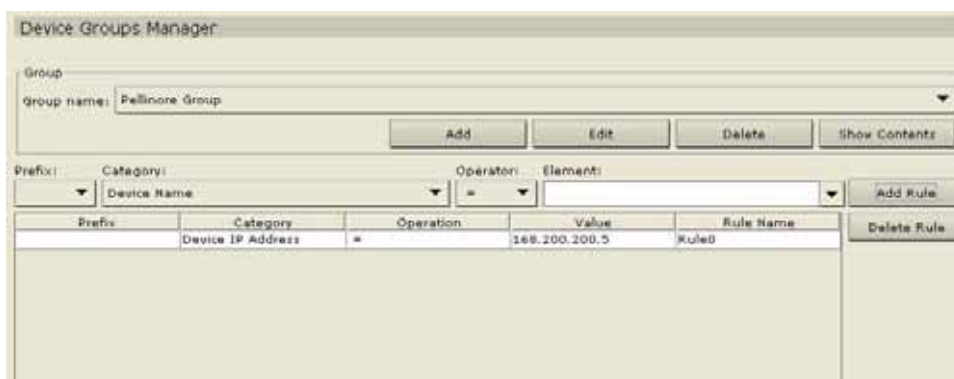


Figure 88 Device Groups Manager Screen

2. Click on the **Group Name** drop-down arrow and select the device group for which you want to set rules.
3. Click on the **Prefix**, **Category**, **Operator**, and **Element** drop-down arrows to set up a rule, and type the name of the rule in the **Rule Name** field.
4. Click **Add Rule**. The new rule appears in the rule table as a short regular expression.

Important: You can combine the application of two or more rules by using operators such as '&' meaning 'and' or '|' (vertical bar that shares the <\> key on your keyboard) meaning 'or.'

Note: When you select a category, make sure you select a proper operator that relates to the element in order for the rule to take effect. For example, if **countries of the world** category is selected, relate it to '=' **operator** to equal only the country you pick as an element of the rule. Devices are grouped according to this rule once added to the system.

1. Click **Validate** and the short regular expression expands into a normal expression of the rule in the lower field of the screen.
2. Click **Update** to update the device group. The new rule is associated with this device group from now on, and any new devices will also comply with rules assigned to this device group.
3. Click **Close** to close the **Device Groups Manager** screen.
4. Repeat steps 1 through 7 to add other rules to device groups.

Delete Device Rule

1. On the **Associations** menu, click **Groups Manager**, and then click **Device Group Manager**. The Device Groups Manager screen appears.

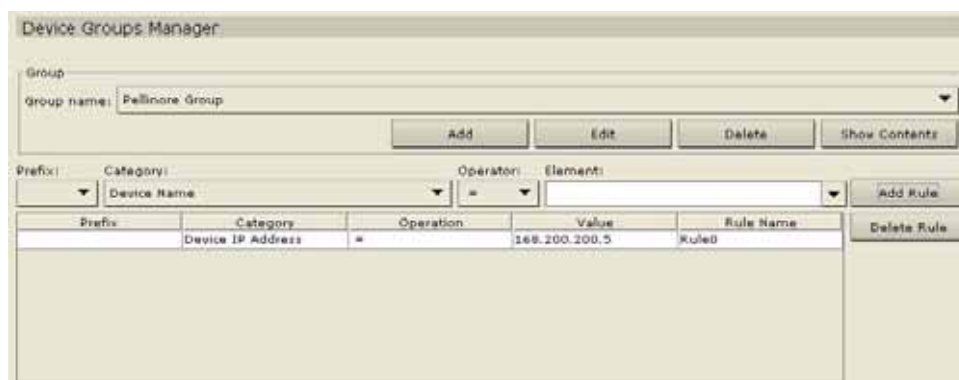


Figure 89 Device Groups Manager Screen

2. Select a rule to be deleted from the rule table and click **Delete Rule**. The Delete Rule window appears.

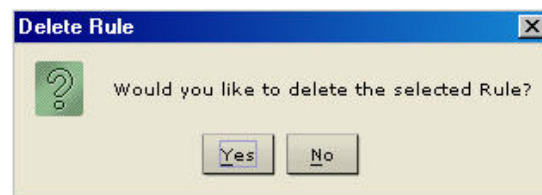


Figure 90 Delete Rule Window

3. Click **Yes** to delete the rule or **No** to close the window.
4. Click **Close** to close Device Groups Manager screen.
5. Repeat steps 1 through 4 to delete other rules.

Search for Devices

CC-SG can search for a device name that satisfies the text entered in the search box. Searches are case-insensitive.

1. Click on the **Devices** tab.

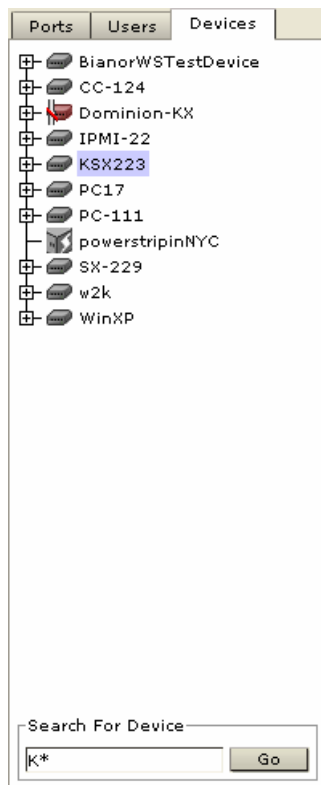


Figure 91 Search for Devices

2. At the bottom of the window, enter a search string in **Search For Device**.
3. Click **Go** or press **ENTER**.

Navigation Tips

- When a device has been found and is highlighted in the Devices tree, use the ↓ and ↑ keys to navigate to the next device.
- When a device is highlighted in the Devices tree, press the **TAB** key to return to the Search For Device box.
- To clear the results and refresh the display in the Devices tree, you can press the **F5** key or click  in the toolbar.

Supported Wildcards

These wildcards are supported:

WILDCARD	DESCRIPTION
?	Indicates any character.
[-]	Indicates a character in range.
*	Indicates zero or more characters.

Examples are as follows:

EXAMPLE	DESCRIPTION
KX?	Locates KX1, and KXZ, but not KX1Z.
KX*	Locates KX1, KX, KX1, and KX1Z.
KX[0-9][0-9]T	Locates KX95T, KX66T, but not KXZ and KX5PT.

Disconnect Users

Administrators can terminate any user's session with a device. This includes users who are performing any kind of operation on a device, such as, connecting to ports, backing up the configuration of a device, restoring a device's configuration, or upgrading the firmware of a device. The administrator, however, will remain logged into CC-SG.

Note: Firmware upgrades and device configuration backups and restores are allowed to complete before the user's session with the device is terminated. All other operations will be terminated immediately.

1. Click on the **Devices** tab.
2. Right-click on the device you want to disconnect one or more users.

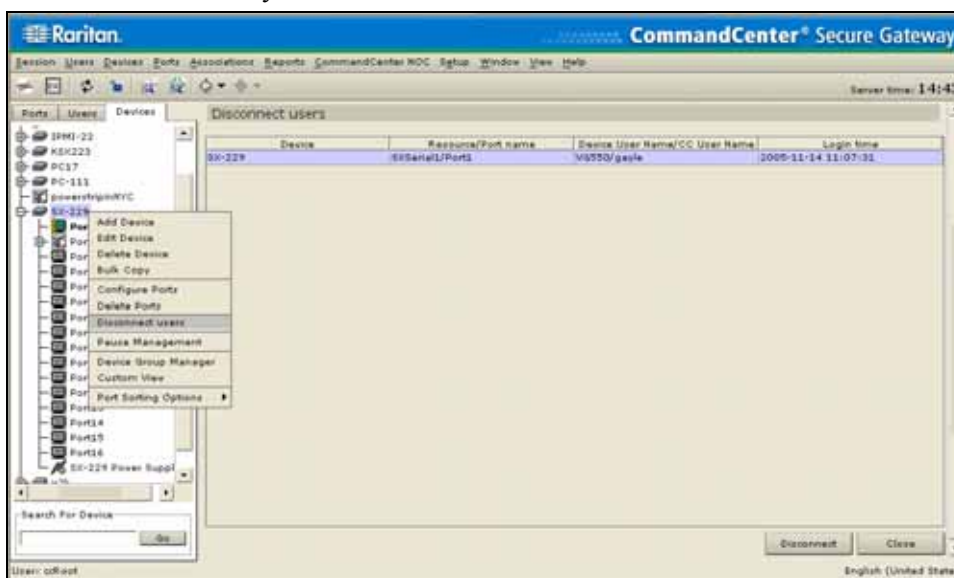


Figure 92 Disconnect Users

3. Click **Disconnect Users**.
4. Highlight one or more users in the Disconnect users panel.
5. Click **Disconnect**.

Note: For Dominion SX devices only, you can disconnect users who are directly logged onto the device as well as those who are connected to the device (port) via CC-SG.

Chapter 6: Configuring Ports and Port Groups

This chapter discusses how to configure and edit ports and port groups. Procedures on how to use ports (connect, disconnect, bookmark ports, search for ports, create views, use port power management, use port chat) are described in Raritan's **CommandCenter Secure Gateway User Guide**.

Port Manager

Port Manager commands allow you to configure, connect to, and disconnect from ports of serial devices, generic devices, IPMI servers, and KVM devices in your CC-SG.

Once configured, CC-SG provides centralized access to the target devices(s) attached to Dominion and IP-Reach units. CC-SG supports Raritan products, as listed in the table below.

RARITAN UNITS	NUMBER OF PORTS	SSL
Dominion SX4	4	Always On
Dominion SX8	8	Always On
Dominion SX16	16	Always On
Dominion SX32	32	Always On
Dominion SX48	48	Always On
Dominion KSX440	8	Always On
Dominion KSX880	16	Always On
Dominion KX116*	16	Always On
Dominion KX216*	16	Always On
Dominion KX232*	32	Always On
Dominion KX416	16	Always On
Dominion KX432	32	Always On
Dominion KX101	1	Always On
IP-Reach	Model Dependent	Always On
P2-SC	Varies	Always On

*Requires DKX firmware support

When you click on the Ports tab, the Ports tree displays information about the Ports connected with CC-SG. Clicking on a port causes the View Port screen to appear. Ports are arranged alphabetically by name, or grouped by availability status. Ports arranged by status are sorted alphabetically within their availability grouping. To switch between arranging methods, right-click on the tree, click **Port Sorting Options**, then click **Sort By Port Name** or **Sort By Port Status**.

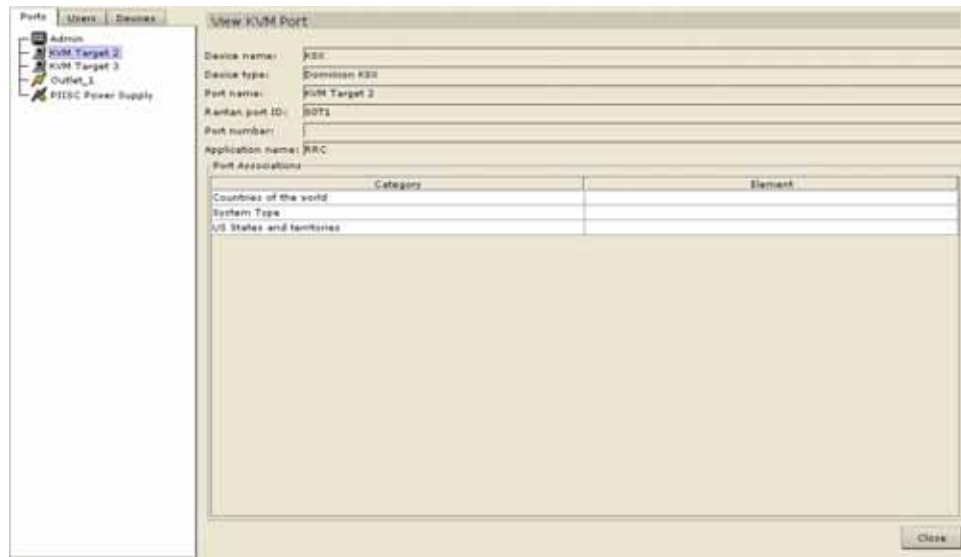


Figure 93 The Ports Tab And View KVM Port Screen

Port Icons

For easier identification, different ports have different icons in the tree. In addition, availability status of each port also has a different icon. For a description of what the icons represent, please see the table below.

ICON	MEANING
	Device available
	Port available
	Ghosted Port – a ghosted port can occur when managing Paragon devices and when a CIM or target server is removed from the system or powered off but a record of it remains.
	KVM port connected – in current user session
	Port paused – because device is paused
	Port unavailable – because device is unavailable
	Port busy – other user connected to port
	Serial port available – not connected
	Serial port connected – in current user session
	Serial port busy – other user connected to port
	Serial port unavailable – device is down and unavailable
	Serial port paused – because device is paused
	Power strip available
	Outlet port available
	Power strip paused
	Outlet port paused

Important! Many of the menu bar commands described in this section can be accessed by right-clicking on a Port icon and selecting a command from the shortcut menu that appears.

Configure Port

Configure a Serial Port

Click on the **Devices** tab and select a serial device from the Devices tree.

1. On the **Devices** menu, click **Port Manager**, and then click **Configure Ports**. The Configure Ports screen appears.

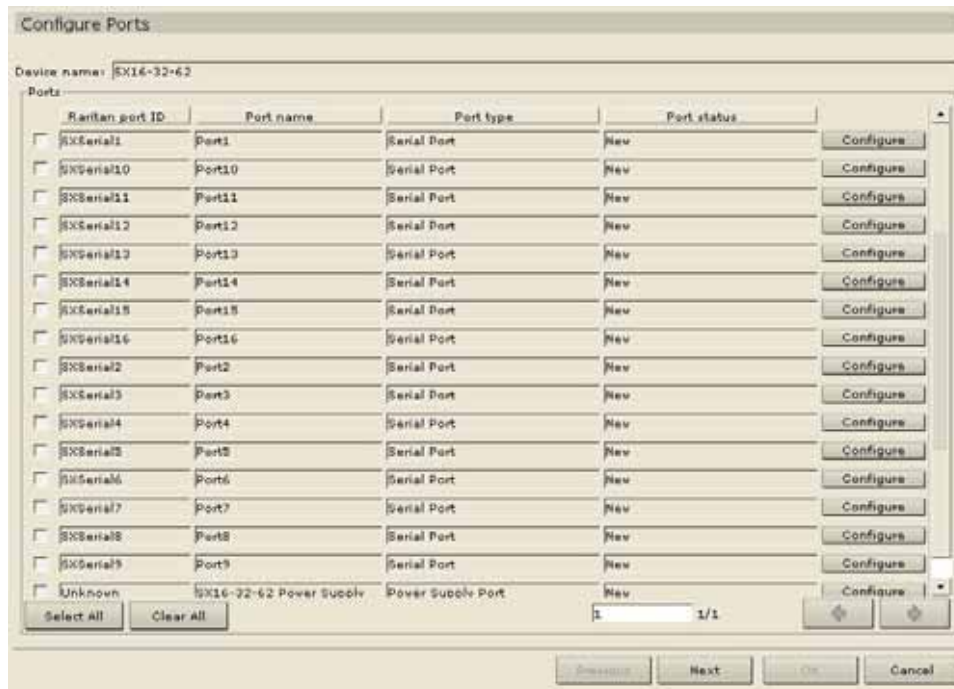


Figure 94 Configure Ports Screen

2. To make ports easier to find, click on a column header to sort the ports by that attribute in ascending order. Click on the header again to sort the ports in descending order.

- Click the **Configure** button that corresponds to the serial port line item you wish to configure. The Configure Serial Port screen appears.

Configure Serial Port

Please select port properties to add.

Port Properties

Device name: SX4-206

Device IP or Hostname: 192.168.53.206

Port number: 2

Raritan port ID: SXSerial2

Port name: Port2

Application name: Raritan Console

Baud rate: 9600

Parity/Data bits: Odd/7

Flow control: Xon/Xoff

Associate Device: None

Port Associations

Category	Element
System Type	
US States and territories	

In-Band Parameters

OK Cancel

Figure 95 Configure Serial Ports Screen

- Type a port name in **Port Name** field. For ease of use, you should name the port after the server that is connected to the port.
- Click on the **Application Name** drop-down arrow and select an application name.
- Click on the **Baud Rate** drop-down arrow and select a rate.
- Click on the **Parity/Data Bits** drop-down arrow and select a parity value.
- Click on the **Flow Control** drop-down arrow and select a flow control value.
- Click on the **Associate Device** drop-down arrow and select a Generic device, IPMI Server, or Powerstrip, which will be associated with this Serial port. When a Generic device is associated with a Serial port, it looks like this in the Devices tree:

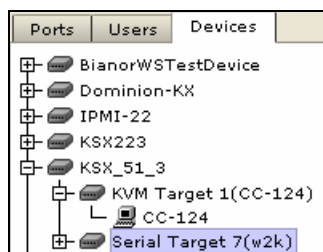


Figure 96 Associated Generic Device with a Serial Port

- Select the associated category and element from the **Port Associations** table.

11. Click **In-Band Parameters** if you want to allow in-band access for this Serial port.

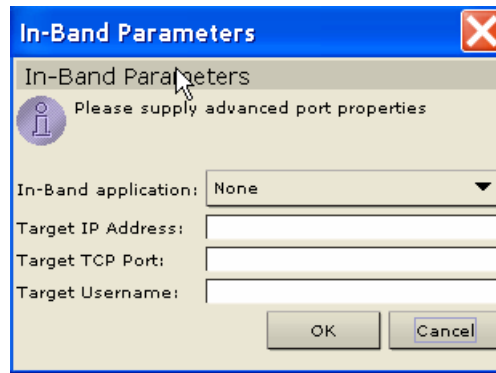


Figure 97 In-Band Parameters

12. Click on the **In-band application** drop-down arrow and select either **RemoteDesktop Viewer**, **SSH Client**, **VNC Viewer**. Type the IP address of the target associated with this port in the **Target IP Address** field, type the port used by the In-band application in **Target TCP Port**, and type a username that is used to login to the in-band application in the **Target Username** field. Click **OK** to save the In-band parameter settings or **Cancel** to exit without saving.
13. Click **OK** to configure the serial port or **Cancel** to exit without configuring. A **Port Configured Successfully** message confirms that the port has been created.
14. Repeat steps 1 through 11 to configure other serial ports.

Note: For KSX power ports and SX serial ports, associating a device with the port is available in the *Configure Serial* screen and not in the *In-Band parameters* screen.

Configure a KVM Port

1. Click on the **Devices** tab and select a KVM device from the Devices tree.
2. On the **Devices** menu, click **Port Manager**, and then click **Configure Ports**. The Configure Ports screen appears.

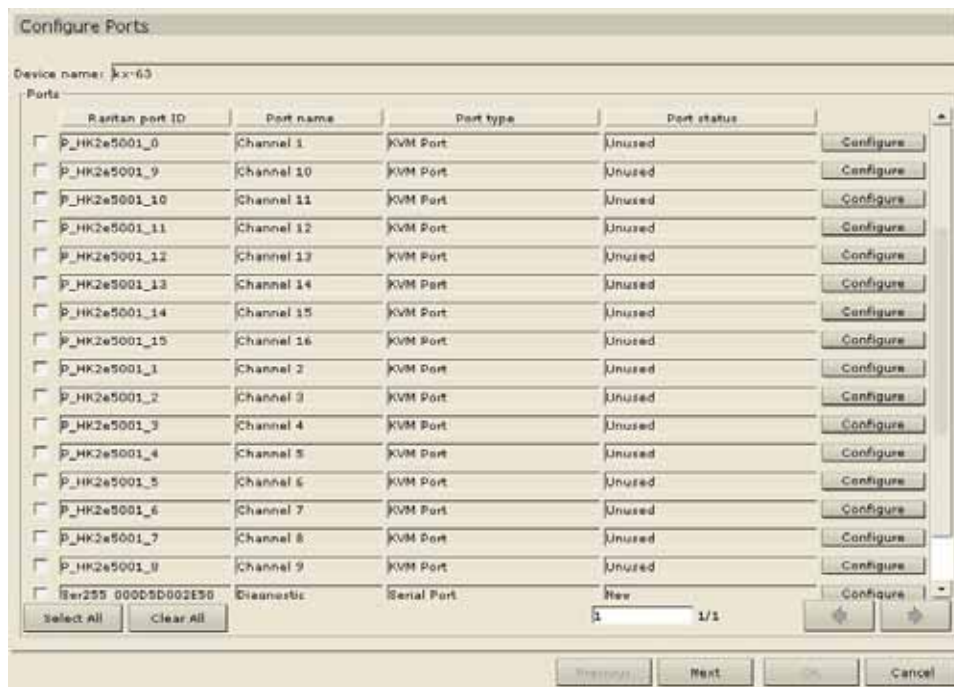


Figure 98 Configure Ports Screen

3. To make ports easier to find, click on a column header to sort the ports by that attribute in ascending order. Click on the header again to sort the ports in descending order.
4. Click the **Configure** button that corresponds to the KVM port line item you wish to configure. The Configure KVM Port screen appears.

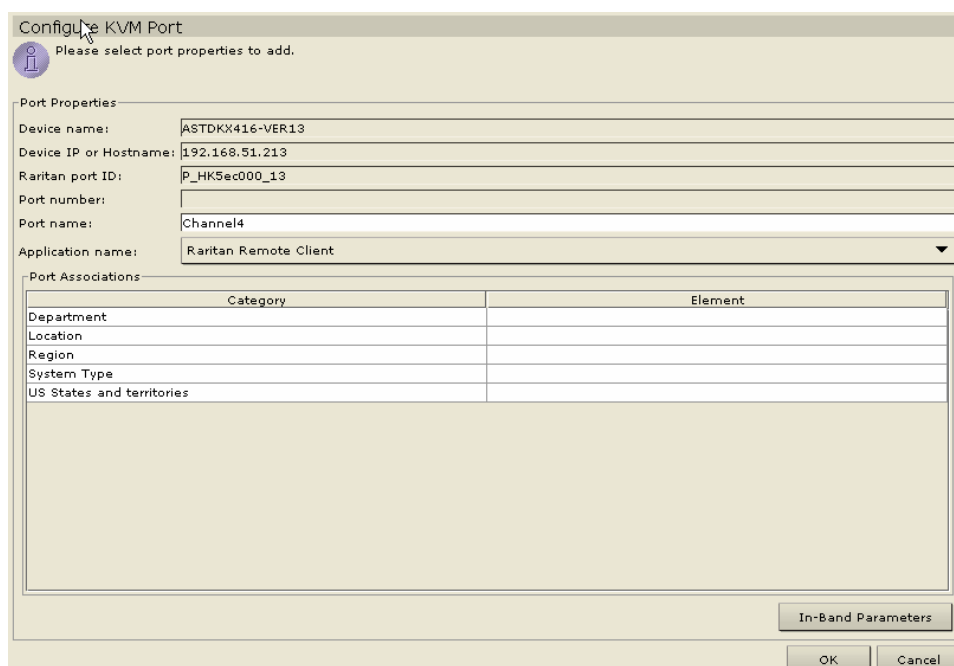


Figure 99 Configure KVM Port Screen

5. Type a port name in the **Port Name** field. For ease of use, you should name the port after the server that is connected to the port.
6. Click on the **Application Name** drop-down arrow and either use the default application as configured in Application Manager or select another application if desired.
7. Select the associated category and element from the **Port Associations** table.
8. Click **In-Band Parameters** if you want to allow in-band access for this KVM port.

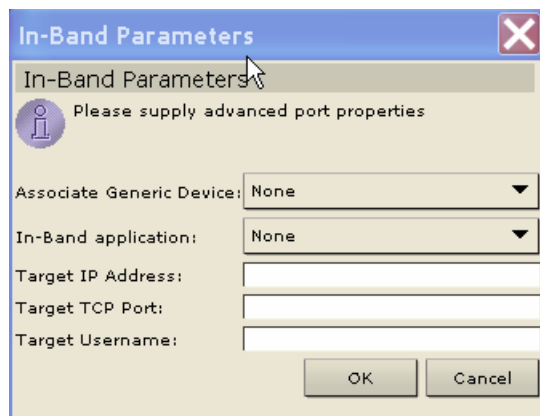


Figure 100 In-Band Parameters

9. Click on the **Associate Generic Device** drop-down arrow and select a Generic device, which will be associated with this KVM port. When a Generic device is associated with a KVM port, it looks like this in the Devices tree:



Figure 101 Associated Generic Device with a KVM Port

10. Click on the **In-band application** drop-down arrow and select either **RemoteDesktop Viewer**, **SSH Client**, **VNC Viewer**. Type the IP address of the target associated with this port in the **Target IP Address** field, type the port used by the In-band application in **Target TCP Port**, and type a username that is used to login to the in-band application in the **Target Username** field. If a target name is supplied, then only a password is required when accessing a target. Click **OK** to save the In-band parameter settings or **Cancel** to exit without saving.
11. Click **OK** to configure the KVM port or **Cancel** to exit with configuring. A **Port Configured Successfully** message confirms that port has been created.
12. Repeat steps 1 through 11 to configure other KVM ports.

Note: You can access a Generic device that is associated with a KVM port by right-clicking on the port in the Ports tree and selecting **Connect**, which uses the application selected, such as Raritan Remote Console, or by selecting **In-band Access**, which uses the in-band application as configured in the In-band Parameters screen.

Configure a Generic Port with In-Band Access

In-band access to Generic devices, such as hubs, Windows servers, CISCO routers, can be managed with one of these in-band applications:

- Windows Remote Desktop (RDP)
- Secure Shell (SSH)
- Virtual Network Computer (VNC)

1. Click on the **Devices** tab and select a Generic device from the Devices tree.
2. On the **Devices** menu, click **Port Manager**, and then click **Configure Ports**. The Configure Ports screen appears.

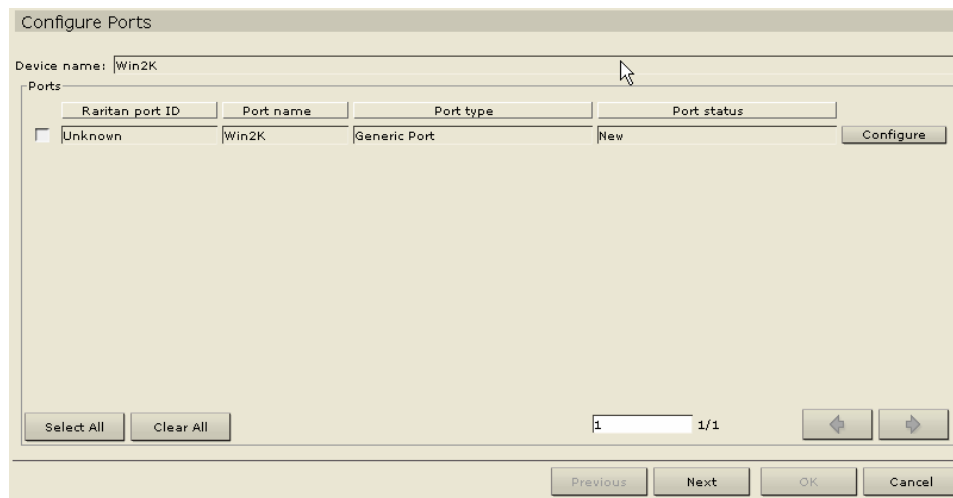


Figure 102 Configure Ports Screen

3. Click the **Configure** button that corresponds to the Generic port line item you wish to configure. The Configure Generic Port screen appears.

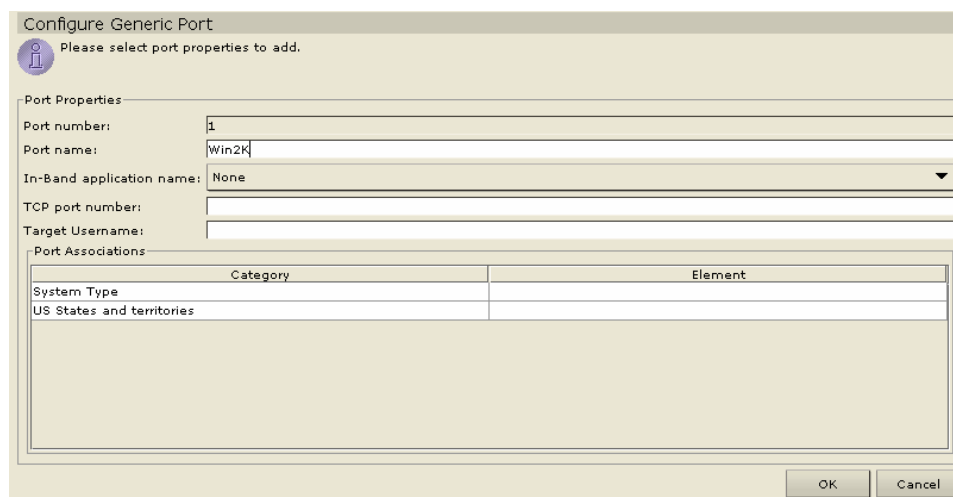


Figure 103 Configure Generic Ports Screen

4. Type a port name in the **Port Name** field. For ease of use, you should name the port after the server that is connected to the port.
5. Click on the **In-Band application name** drop-down arrow and select an in-band application, such as SSH Client, VNC Viewer, or RemoteDesktop Viewer to manage the device.
6. Type a **TCP port number** that the application will use as a Start-up parameter.

7. Type a **Target Username** that the application will use as a Start-up parameter. If a target name is supplied, then only a password is required when accessing a target.
8. Select the associated category and element from the **Port Associations** table.
9. Click **OK** to configure the Generic port or **Cancel** to exit with configuring. A **Port Configured Successfully** message confirms that port has been created.
10. Repeat steps 1 through 9 to configure other Generic ports.

Configure an Outlet Port

Outlet ports can be configured for PowerStrip devices and IPMI servers.

1. Click on the **Devices** tab and select a PowerStrip device from the Devices tree.
2. On the **Devices** menu, click **Port Manager**, and then click **Configure Ports**. The **Configure Ports** screen appears.

Configure Ports

Device name: powerstripinNYC

	Raritan port ID	Port name	Port type	Port status	
☐	Unknown	Outlet_1	Outlet Port	New	Configure
☐	Unknown	Outlet_2	Outlet Port	New	Configure
☐	Unknown	Outlet_3	Outlet Port	New	Configure
☐	Unknown	Outlet_4	Outlet Port	New	Configure
☐	Unknown	Outlet_5	Outlet Port	New	Configure
☐	Unknown	Outlet_6	Outlet Port	New	Configure
☐	Unknown	Outlet_7	Outlet Port	New	Configure
☐	Unknown	Outlet_8	Outlet Port	New	Configure

Select All Clear All 1 1/1

Figure 104 Configure Ports Screen for Powerstrip Device

Configure Ports

Device name: IPMI-22

	Raritan port ID	Port name	Port type	Port status	
☐	Unknown	IPMI-22 Power Supply	Power Supply Port	New	Configure
☐	Unknown	KSX223 Port 1	Outlet Port	New	Configure

Figure 105 Configure Ports Screen for IPMI Server

- Click the **Configure** button that corresponds to the outlet port line item you wish to configure. A **Configure Outlet Port** screen appears.

Configure Outlet Port

Please select port properties to add.

Device name: PS18

Port number: 10

Port name: Outlet_10

Associated port: None

Category	Element
Countries of the world	
System Type	
US States and territories	

OK Cancel

Figure 106 Configure Outlet Port Screen

- Type the port name in the **Port Name** field. For ease of use, you should name the port after the server that is connected to the port.
- If you want to associate this port with another port, click on the **Associated Port** drop-down arrow and select a port name. For example, an outlet of an IPMI server may be connected to a channel of a Raritan KX device.
- Click **OK** to configure the outlet port or **Cancel** to exit without configuring. A **Port Configured Successfully** message confirms that outlet port has been created.
- Repeat steps 1 through 6 to configure other outlet ports.

Delete Ports

Delete a port to remove the port entry from the Ports tree and **Cancel** all accessibility of the remote target device.

1. Click on the **Ports** tab and select a port to be deleted.
2. On the **Devices** menu, click **Port Manager**, and then click **Delete Port**. The **Delete Port** screen appears.



Figure 107 Delete Port Screen

3. Click **OK** to delete the port or **Cancel** to exit without deleting. A **Port Deleted Successfully** window confirms that port has been deleted.
4. Repeat steps 1 through 3 to delete other ports.

Bulk Copy

To save time, use the Bulk Copy command to duplicate Port names or associations to other ports.

1. Click on the **Ports** tab and select a port whose data you want to copy to another.
2. On the **Ports** menu, click **Bulk Copy**. The **Bulk Copy** screen appears.

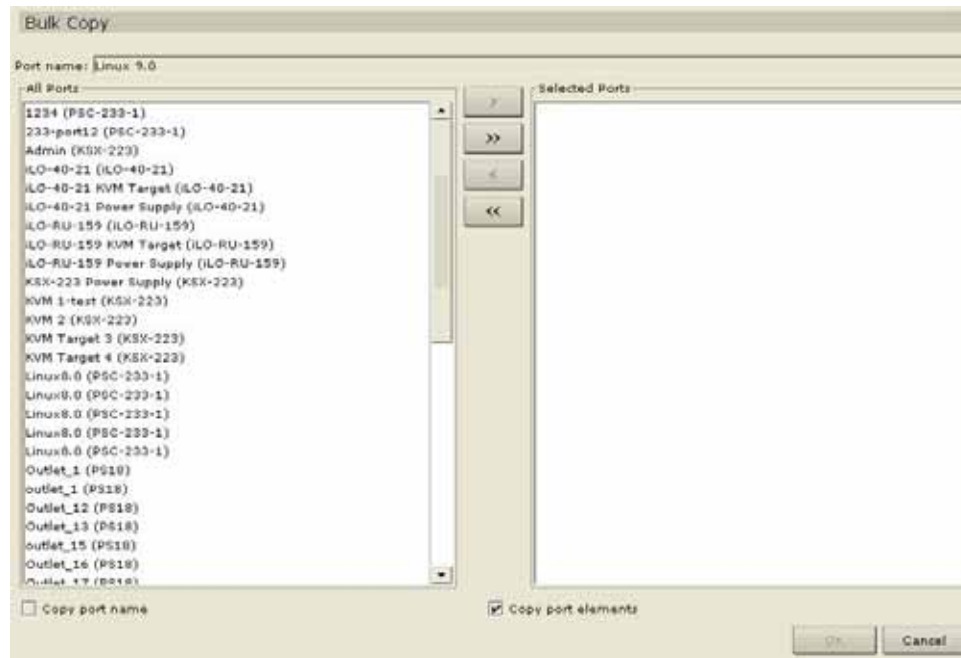


Figure 108 Bulk Copy Screen

3. In the **All Ports** list select the port name(s) that will be adopting the profile of the port listed in the **Port Name** field above.
4. Click > to move a port name to the **Selected Ports** list.
5. To remove a port name from the **Selected Ports** list, click on the name and click < to move it back to the **All Ports** list.
6. Click **OK** to copy port properties or **Cancel** to exit without copying. A **Port Copied Successfully** message confirms that the port profile has been copied.
7. Repeat steps 1 through 6 to make other bulk copies of port properties.

Edit Port

Edit a Serial Port

1. Click on the **Ports** tab and select a serial port to be edited.
2. On the **Ports** menu, click **Edit Port**. The **Edit Serial Port** screen appears.

Edit Serial Port

Please select port properties to add.

Port Properties

Port number: Unknown

Raritan port ID: Ser_2

Port name: Serial Target 3

Application name: Raritan Remote Client

Baud rate: 9600

Parity/Data bits: None/8

Parity check: ☒ Enable

Recv/Xmit pace: ☒ Xon/Xoff

H/W flow control: ☒ Enable

Port Associations

Category	Element
adf	
System Type	
US States and territories	

In-Band Parameters

Figure 109 Edit Serial Port Screen

3. Type the new port name in the **Port Name** field.
4. Click on the **Application Name** drop-down arrow and select a new application name.
5. Click on the **Baud Rate** drop-down arrow and select a new rate.
6. Click on the **Parity/Data Bits** drop-down arrow and select a new value.
7. Click on the **Parity Check** checkbox to enable or disable.
8. Click on the **Recv/Xmit Pace** check box to enable or disable **Xon/Xoff**.
9. Click on the **H/W Flow Control** check box to enable or disable.
10. Click on the **In-band Parameters** if you want to change the in-band parameters.
11. Select a new category and element from the **Port Associations** table.
12. Click **OK** to edit the port or **Cancel** to exit without saving the changes. A **Port Updated Successfully** confirms that port has been updated.
13. Repeat steps 1 through 12 to edit other ports.

Edit a KVM Port

1. Click on the **Ports** tab and select a KVM port to be edited.
2. On the **Ports** menu, click **Edit Port**. The **Edit KVM Port** screen appears.

Edit KVM Port

Please select port properties to add.

Raritan port ID: S0T1

Port number:

Port name: KVM Target 2

Application name: RRC

Port Associations

Category	Element
System Type	US States and territories

OK Cancel

Figure 110 Edit KVM Port Screen

3. Type a new port name in the **Port Name** field.
4. Click on the **Application Name** drop-down arrow and select an application from the list.
5. Select a new category and element from the **Port Associations** table.
6. Click **OK** to edit the port or **Cancel** to exit without saving the changes. A **Port Updated Successfully** confirms that port has been updated.
7. Repeat steps 1 through 7 to edit other ports.

Edit a Generic Port

1. Click on the **Ports** tab and select a Generic port to be edited.
2. On the **Ports** menu, click **Edit Port**. The **Edit Generic Port** screen appears.

Edit Generic Port

Please select port properties to add.

Port Properties

Port number: 1

Port name: Windows XP

In-Band application name: None

TCP port number:

Target Username:

Port Associations

Category	Element
System Type	
US States and territories	

OK Cancel

Figure 111 Edit Generic Port Screen

3. Type a new port name in the **Port Name** field.
4. Click on the **In-band application name** drop-down arrow and select an application from the list.
5. Type a new port number in the **TCP port number** field.
6. Type a new username in the **Target Username** field.
7. Select a new category and element from the **Port Associations** table.
8. Click **OK** to edit the port or **Cancel** to exit without saving the changes. A **Port Updated Successfully** confirms that port has been updated.
9. Repeat steps 1 through 8 to edit other ports.

Port Group Manager

Add Port Group

1. On the **Associations** menu, click **Groups Manager** and then click **Port Group Manager**. The **Port Groups Manager** screen appears.

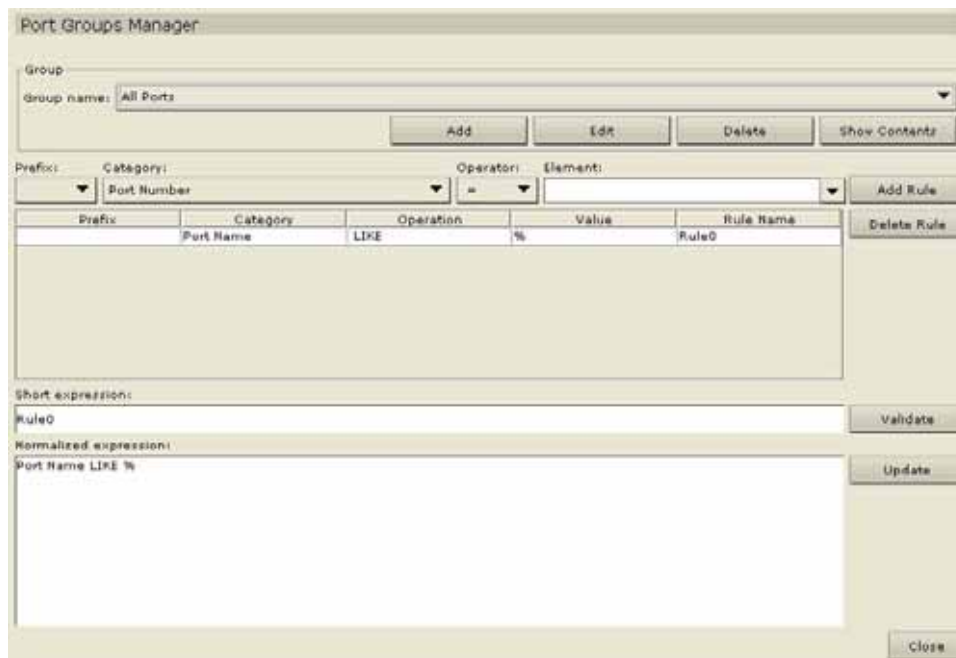


Figure 112 Port Groups Manager Screen

2. Click **Add** in the **Group** panel to add a new group. The **Add Port Group** window appears.



Figure 113 Add Port Group Window

3. Type the name for the new Port Group in the **Enter Name for Port Group** field.
4. Click **OK** to add the new group or **Cancel** to close the window.
5. Click **Close** to close **Port Groups Manager** screen.
6. Repeat steps 1 through 5 to add other port groups.

Edit Port Group

1. On the **Associations** menu, click **Groups Manager** and then click **Port Group Manager**. The **Port Groups Manager** screen appears.
2. Click on the **Group Name** drop-down arrow and select a group to edit. Click **Edit** in the **Group** panel. The **Edit Port Group** window appears.



Figure 114 Edit Port Group Window

3. Type a new name for the group in the **Enter New Name for Port Group** field.
4. Click **OK** to update the change or **Cancel** to close the window.
5. Click **Close** to close the **Port Groups Manager** screen.
6. Repeat steps 1 through 5 to edit other port groups.

Delete Port Group

1. On the **Associations** menu, click **Groups Manager** and then click **Port Groups Manager**. The **Port Groups Manager** screen appears.
2. Click on the **Group Name** drop-down arrow and select a group to delete from the list. Click **Delete** to delete the group. The **Delete Port Group** window appears.



Figure 115 Delete Port Group Window

3. Click **Yes** to delete the port group or **No** to close the window.
4. Click **Close** to close the **Port Groups Manager** screen.
5. Repeat steps 1 through 4 to delete other port groups.

Chapter 7: Adding Users and User Groups

User Manager commands are listed in the Users menu and allow you to define the CC-SG user list and assign user privileges for performing various functions. CC-SG maintains a centralized user access list. Only an Administrator (a user with Administrator privileges) can manage user accounts.

Important! Many of the menu bar commands can be accessed by right-clicking on a User icon in the Selection tree (on the left side of your CC-SG window) and choosing a command from the shortcut menu that appears.

Add User

1. Right-click on a user group in the Users tree and select **Add User**. The **Add User** screen appears.

Figure 116 Add User Screen

2. Type the user's name in the **Username** field (4-16 characters, alphanumeric characters or underscores, no spaces for locally authenticated users and no length restriction for users authenticated remotely).
3. Check the **Remote Authentication** check box only if the user should be authenticated by TACACS+, Active Directory, RADIUS, or LDAP (please see **Chapter 9: Configuring Remote Authentication** for additional information).

Note: Checking the **Remote Authentication** box implies that a remote server is being used for authentication. If so, a local password is not required.

4. For local CC-SG authentication only, type the new password into the **Password** field (6-16 characters, alphanumeric characters and underscores, no spaces).
5. Re-type password in **Retype Password** field.
6. The dial back number in the **Dial Back Number** field is configured under the **Modem** tab in **Configuration Manager**—see **Modem Configuration** in **Chapter 12: Advanced Administration**.
7. Check the **Login Enabled** check box to authenticate against the system (if not, user cannot enter the system).

8. Check the **Force Change Password on Next Login** check box if you want this user to be forced to change password the next time he or she logs in to CC-SG.
9. Check the **Force Change Password Periodically** check box if you want this user to have to change his or her password from time to time. Either type the expiration period (in days) for this user's password in the **Expiration Period** field or select a date in **Expiration Date**. Selecting one method automatically performs the calculation for the other.
10. If blank, check the **Force strong password check** checkbox if you want to enforce strong passwords for this particular user. Strong passwords is a system-wide setting that is configured in Security Manager—see **Configure Security** in **Chapter 12: Advanced Administration** for additional information. If strong passwords are enabled in Security Manager, then you cannot change the setting in this screen.
11. Type an email address for the user.
12. By default, the user will be added to the user group that is selected in the Users tree. If you do not want the user added to the group, deselect the **Add to group:** checkbox, which will add the user to the **Users Not in Group** user group. The user can then be moved to the desired user group.
13. Click **OK** to add this user to the system, or **Cancel** to exit without saving. A **User Created Successfully** message indicates the user has been added to the system.

Note: If New User submission fails, an error message appears. Possible explanations include:

- ▶ New password is too short. Password should be at least six characters in length.
 - ▶ User Name or Password does not conform to requirements as stated above.
 - ▶ Password and Confirm Password do not match.
 - ▶ A user account with same User Name already exists on CC-SG.
-

14. Repeat steps 1 through 13 to add other users.

Edit User

This command allows you, as Administrator, to edit a user's parameters.

1. Click on the **Users** tab. In the Users tab area, a Group icon shows multiple figures, and a User icon appears as a single person; click on the + sign before a group name to expand and view all users within it. Select a user from the Users tree.
2. On the **User** menu, click **Edit User**. The **Edit User** screen appears.

Figure 117 Edit User Screen

3. Check the **Login enabled** check box to authenticate the user against the system (if not, user cannot enter the system).
4. Check the **Force Change Password on Next Login** check box if you want this user to be forced to change password the next time he or she logs into CC-SG.

5. Check the **Force Change Password Periodically** check box if you want this user to have to change his or her password from time to time and specify an expiration period for this user's password in the **Expiration Period** field.
6. Check the **Force strong password check** checkbox if you want to enforce strong passwords for this user—see **Strong Password Rules** in **Chapter 12: Advanced Administration** for additional information.
7. Type an email address for the user.
8. Click **OK** to submit the changes or **Cancel** to exit without saving. An **Updated Successfully** message confirms the edits were submitted.
9. Repeat steps 1 through 8 to edit other users.

Change User Password

This command allows you to change any user's password.

1. Click on the **Users** tab and select a user from the Users tree
2. On the **User** menu, click **Change User Password**. The **Change User Password** screen appears.



Figure 118 Change User Password Screen

3. Type the new password in the **Password** field.
4. Re-type password in the **Retype Password** field.
5. Click **OK** to change user password or **Cancel** to exit without saving. A **User Password Updated Successfully** message confirms the password has been changed.
6. Repeat steps 1 through 5 to change other users' passwords.

Note: For strong passwords, minimum length is 6 characters. For non-strong passwords, minimum length is 4 characters. See section **Configure Security** in **Chapter 12: Advanced Administration** for additional information.

Change Own Password

For security reasons, you may choose to change your own password.

1. On the **Session** menu, click **Change My Profile**. The **Change My Profile** screen appears.

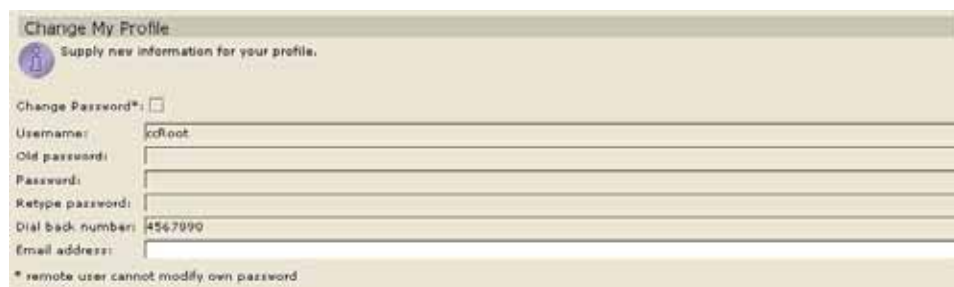


Figure 119 Change My Profile Screen

2. Type your old password in the **Old Password** field.
3. Type your new password in the **Password** field. You cannot re-use your old password.
4. Re-type your password in the **Retype Password** field.
5. Click **OK** to change your password or **Cancel** to exit without saving. A **User Profile Updated Successfully** message confirms that your password has been changed.
6. Repeat steps 1 through 4 to change your password whenever necessary.

Note: For strong passwords, minimum length is 6 characters. For non-strong passwords, minimum length is 4 characters. See section **Configure Security** in **Chapter 12: Advanced Administration** for additional information.

Delete User

As an Administrator, you can remove a user account that is no longer needed.

1. Click on the **Users** tab and select a user from the Users tree.
2. On the **User** menu, click **Delete User**. The **Delete User** screen appears.



Figure 120 Delete User Screen

3. Click **OK** to delete the user or **Cancel** to exit without deleting. A **User Deleted Successfully** message confirms that user has been deleted.
4. Repeat steps 1 through 3 to delete other users.

Note: A user cannot be deleted if currently logged into CC-SG.

Logoff User(s)

Use this command to disconnect any logged-in user from CC-SG.

1. Click on the **Users** tab and select a user from the Users tree.

Note: To select more than one user, hold the **CTRL** key and click on additional users.

2. On the **Users** menu, click **Logoff User(s)**. The **Logoff Users** screen appears.

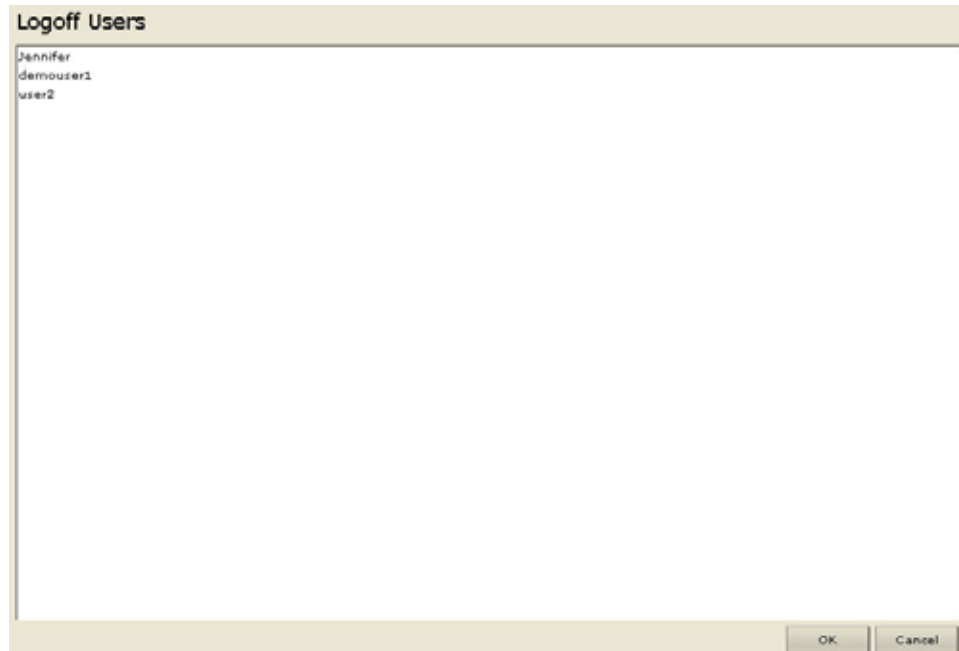


Figure 121 Logoff Users Screen

3. Click **OK** to disconnect the users or **Cancel** to exit without disconnecting users. A **User Logged off Successfully** message confirms that the users have been logged off.

Bulk Copy

To save time, use the Bulk Copy command to duplicate user profiles or port assignments when creating new users.

1. Click on the **Users** tab and select a user from the Users tree whose properties you want to copy to another user(s).
2. On the **Users** menu, click **Bulk Copy**. The **Bulk Copy** screen appears.

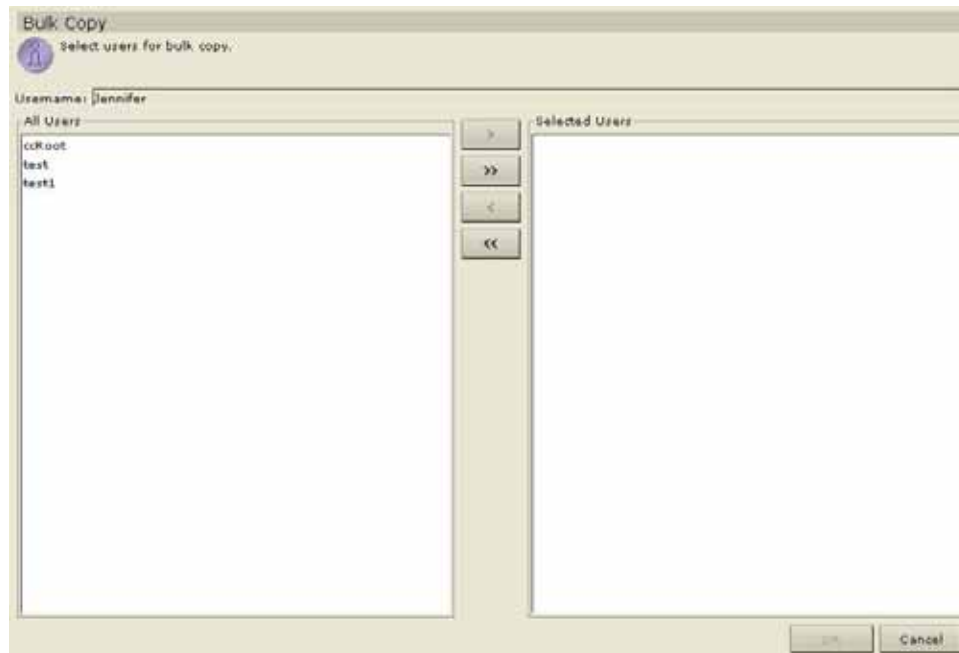


Figure 122 Bulk Copy Screen

3. In the **All Users** list select the user name(s) that will be adopting the profile of the user listed in the **Username** field.
4. Click > to move a user name to the **Selected Users** list.
5. To remove a user name from the **Selected Users** list, click on the name and click < to move it back to the **All Users** list.
6. Click **OK** to copy user properties or **Cancel** to exit without copying. A **User Copied Successfully** message confirms that the user profile has been copied.
7. Repeat steps 1 through 6 to make other bulk copies of user properties.

Add User to Group

To manage users with similar privileges, you can assign them to groups. When you add a user to any group, you are assigning the group's privileges to that user (please see the section **Add User Group** in this chapter for more information about groups).

1. Click on the **Users** tab and select a group (the Group icon displays multiple people and a User icon displays a single person).
2. On the **Users** menu, click **Add User To Group**. The **Add User To Group** screen appears.

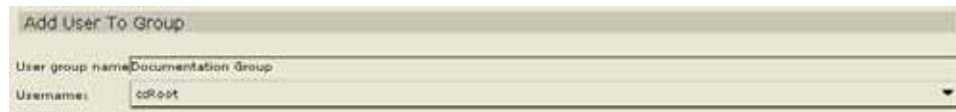


Figure 123 Add User To Group Screen

3. Click on the **Username** drop-down arrow and select a user from the list to add to the group shown in the **User Group Name** field.
4. Click **OK** to add the selected user to the group or **Cancel** to exit without adding. An **Added Successfully To User Group** message confirms that the user has been added to a group.
5. Repeat steps 1 through 4 to add more users to this or to other groups.

Delete User from Group

This command removes a user from a specific group, but not from the system. If a user is not assigned to any other group, that user is moved to **Users Not In Group**, a non-specific category shown at the base of the Users tree.

1. Click on the **Users** tab and select a user to be deleted.
2. On the **Users** menu, click **Delete User From Group**. The **Delete User From Group** screen appears.



Figure 124 Delete User From Group Screen

3. Click **OK** to delete the user or **Cancel** to exit without deleting. A **Deleted Successfully From Group** message confirms that the user has been deleted from the group.
4. Repeat steps 1 through 3 to delete other users from this or other groups.

Default User Groups

A CC-SG is shipped with these default user groups:

- **System Administrators**—user group in which **ccroot** resides. The account **ccroot** is a special type of super-user Administrator, which is always authenticated locally by CC-SG. Users in this group have all privileges as listed in **Appendix D: User Group Privileges**, but the privileges cannot be changed. Users in this group can also manage (add, edit, delete) users and user groups. Policies can be applied to users in this group to provide access rights to ports.
- **CC Users**—initially has only the **Ports Access** privilege, but the privileges can be changed in this group. Policies can be applied to this group to provide access rights to ports.

Note: The **Users Not in Group** is technically not a user group but can be considered as a “holding area” for users until they are moved into another group.

Add User Group

Use the Add User Group command to create specific groups and assign them different privileges, depending on the needs of your work environment. Groups can help you keep your system organized.

Assign privileges, or features, to Groups upon creating them. These **Select Privileges** are privileges of either a command type or an event type. Command type privileges permit users to see and execute commands. Event type privileges permit users to view events in the Ports and Devices trees.

Users inherit the features privileges assigned to the group to which they belong. No user can have any rights other than those assigned to the group. As an example, if a group is assigned the **User Management** feature, all users in that group can see and execute the User Manager commands in the **Users** menu: **Add User**, **Edit User**, **Change User Password**, etc.

In order to see Ports and Devices trees, a user group has to be assigned the **Device and Port Management** feature. To view other events that occur in the system, those privileges must be selected upon Adding or Editing a User Group. This chapter explains how to assign privileges to groups; please see **Appendix D: User Group Privileges** for more information on what each privilege means.

1. On the **Users** menu, click **Add User Group**. The **Add User Group** screen appears.

Has It	Name
☐	CC Setup And Control
☐	Device And Port Management
☐	Device Configuration And Upgrade Management
☐	Ports Access

Figure 125 Add User Group Screen

2. Type the group name in the **User Group Name** field (1-16 characters, alphanumeric characters and underscores).
3. Type the group description (for example, based on department, region, or assignment) in the **Description** field.
4. In the **Select Privileges** section, check the check box(es) in the **Has it** column to assign the specific privilege line items to the group. The **Type** column indicates whether the feature is a Command type feature or an Event type feature (please see **Appendix D: User Group Privileges** for more information).
5. Click **OK** to add the group or **Cancel** to exit without saving. A **User Group Created Successfully** message confirms that a group has been created.
6. Repeat steps 1 through 5 to add other groups.

Edit User Group

This command allows you to rename group and modify its Features.

Important: Please remember that you must be an Administrator to modify User Groups. The category Users Not In Group cannot be modified. Members of that group have observation rights only.

1. Click on the **Users** tab and select a group.
2. On the **Users** menu, click **Edit User Group**. The **Edit User Group** screen appears.

Has It	Name
☒	CC Setup And Control
☒	Device And Port Management
☒	Device Configuration And Upgrade Management
☒	Ports Access

Figure 126 Edit User Group Screen

3. Type a new group name in the **User Group Name** field.
4. Type a new description in the **Description** field.
5. Check the **Select Privileges** check box(es) in the **Has it** column to assign the specific feature line items to the group (please see **Appendix D: User Group Privileges** for more information).
6. Click **OK** to update the group features or **Cancel** to exit without saving. A **Group Updated Successfully** message confirms that group features have been updated.

Apply (Edit) User Group Policies

Groups can be assigned policies, or permissions, that allow them to view and/or control devices and ports. Depending on which policies are assigned to them, groups might have: No Rights, Some Rights, Control Rights, or Full Administration Rights. Policies can be set up using **Policy Manager** commands, as described in the section **Policy Manager**, later in this chapter.

1. Click on the **Users** tab and select a group.
2. On the **User** menu, click **Edit User Group Policies**. The Edit User Group Policies screen appears.

Figure 127 Edit User Group Policies Screen

3. Click on a line item in the **Policies** list (under the All Policies panel) that you wish to assign to the group. Scroll up or down to view all policies in this list. Click on the Day(s) check boxes to select which days of the week the policy should be assigned.
4. Click **Add** to add the policy to the Selected Policies panel and assign it to the group.
5. To remove an assigned policy from the Selected Policies list, select the policy line item and click **Delete**.
6. Click **OK** to add the policy or policies to the group or **Cancel** to exit without editing. A **User Group Policies Updated Successfully** message confirms that policies have been updated.
7. Repeat steps 1 through 6 to edit other groups' policies.

Delete User Group

This command allows you to remove a group name from the system. Users from the deleted group will be re-assigned to the category **Users Not In Group**, displayed at the base of the Users tree.

1. Click on the **Users** tab and select a group.
2. On the **User** menu, click **Delete User Group**. The Delete User Group screen appears.



Figure 128 Group Delete User Group Screen

3. Click **OK** to delete the group or **Cancel** to exit without deleting. A **User Group Deleted Successfully** message confirms that group has been deleted.
4. Repeat steps 1 through 3 to delete other groups.

Assign Users to Group

Use this command to assign users who are members of one group to a different group. Users can be members of more than one group.

1. Click on the **Users** tab and select a group to which you want to add users.
2. On the **User** menu, click **Assign Users To Group**. The Assign Users in Group screen appears.

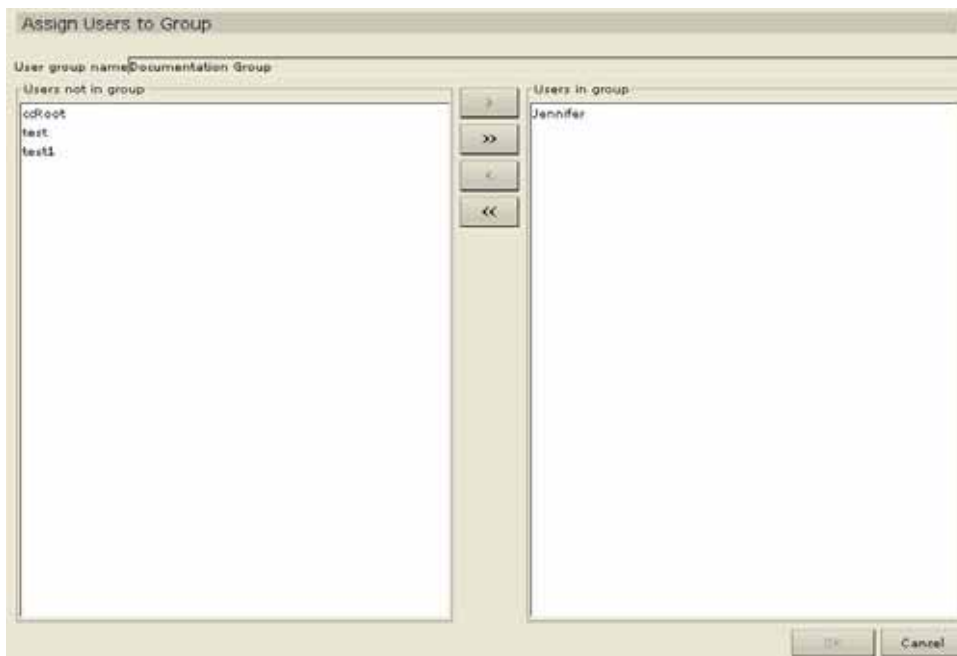


Figure 129 Assign Users in Group Screen

3. All users in the system are listed in the **Users not in group** list. Select a user or users to assign to the group listed in the **User group name** field.
4. Click **>** to add the user name to the **Users in group** list.
5. To remove any user names from the **Users in group** list, select the user names and click **<**.

6. Click **OK** to assign users to the group or **Cancel** to exit without saving. A **Users Assigned Successfully** message confirms that users have been assigned.
7. Repeat steps 1 through 6 to assign users to other groups.

Search for Users

CC-SG can search for a user that satisfies the text entered in the search box. Searches are case-insensitive.

1. Click on the **Users** tab.

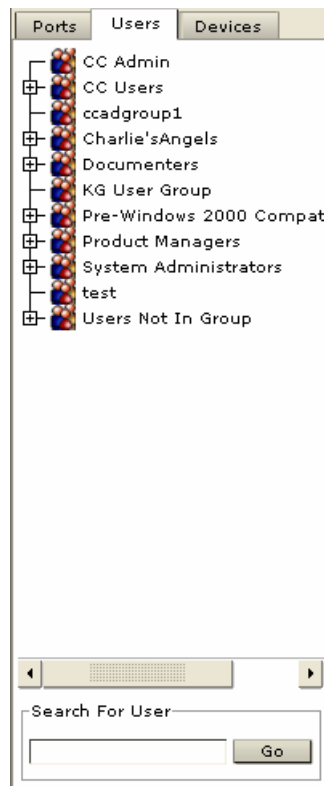


Figure 130 Search for Users

2. At the bottom of the window, enter a search string in **Search For User**.
3. Click **Go** or press **ENTER**.

Navigation Tips

- When a user has been found, the user is displayed in the Users tree. Use the **↓** and **↑** keys to navigate to the next user.
- When a user is highlighted in the Users tree, press the **TAB** key to return to the Search For User box.
- To clear the results and refresh the display in the Users tree, you can press the **F5** key or click  in the toolbar.

Supported Wildcards

These wildcards are supported:

WILDCARD	DESCRIPTION
?	Indicates any character.
[-]	Indicates a character in range.
*	Indicates zero or more characters.

Example:

EXAMPLE	DESCRIPTION
root?	Locates root1, and rootN, but not root1N.
ccroot*	Locates ccroot2SX, ccroot12KX.
admin[0-9][0-9]	Locates admin11, but not admin112.

Chapter 8: Creating Policies

Controlling User Access with Policies

Using policies to control user access to ports is entirely optional. You could decide to assign all users to the default **System Administrators** user group, which grants full access to all configuration tasks, devices, ports, target systems and servers.

If you do want to control user access to target servers, you need to create user groups and apply policies to them. If you used the Association Wizard, policies were automatically created for you. First you create user groups and then you apply the default policies to the user groups. At that point, you may want to add individual users to the user group so they are governed by the policies.

In summary: *Create User Group>Apply Existing Policy to User Group>Add Users*

If you did not use the Association Wizard, you need to do the following: First you create user groups, then port groups, then policies, and lastly you apply the policies to the user groups. At that point, you can add individual users to the user group so they are governed by the policies. This method allows you to choose a policy you created as opposed to using the default policy created in the Association Wizard.

In summary: *Create User Group>Create Port Group>Create Policy>Apply Policy to User Group>Add Users*

Policy Terminology

You should read the following definitions to understand how they relate to policies:

- **Policies**—define the permissions, type of access, and to which ports and/or devices a user group has access to. Policies are applied to a user group and have several control parameters to determine the level of control, such as date and time of access.
- **Port Groups**—define ports that are accessible to a user. Port groups are used when creating a policy to control access to the ports in the group.
- **User Groups**—are a set of users that share the same level of access and privileges. For example, the default user group **System Administrators** has full access to all configuration tasks and target hosts and servers. All other user groups have restricted CC-SG access and should typically be employed for users who need port access only to a particular set of devices or target servers and systems.

User Groups

User groups are used to define a group of users and CC-SG privileges they possess. When a user logs on, they will see the CC-SG interface. The user group privileges define what the user can do with CC-SG. The default **System Administrators** user group has access to all managed devices and ports as well as all CC-SG functions.

A user may just be allowed access to ports and devices or have access to all of the tools of CC-SG. For example, you could create a user group of UNIX administrators and just allow them access to ports that connect to UNIX target servers. Or, you could also create a group of system administrators and give access to CC-SG tools as well as devices and ports.

You should decide upfront what user groups need to be created and what servers users in the group have access to. The following is an example of a User Group implementation that could be created from our sample configuration:

USER GROUP	ACCESS TO...
Window admin group	All Windows servers.
NYC Unix admin group	All New York City Unix servers.
IT admin group	All IT servers.

Port Groups

As you add ports, you link them to your predefined categories and elements. When you create a port group, you will use your categories and elements to define which ports go in each group. You could create a port group of all UNIX ports only. This could be used to only allow UNIX administrators access.

When you use the Association Wizard to define categories and elements, a default port group is automatically created for each element. For example, New York City is an element of the Location category. Therefore, a New York City Ports group was created with one rule, Location = New York City. Additional rules, for example, PortType = UNIX, could be added by using the **Port Group Manager**. To control access to this group of ports, you could create a policy to include this port group, and apply it to the NYC Unix admin user group.

Device Groups

As you add devices, you link them to your predefined categories and elements. When you create a device group, you will use your categories and elements to define which devices go in each group. You could create a device group of all devices that have an IP address starting with 192.168. This could be used to only allow administrators access to those devices on a particular subnet. To control access to this group of devices, you could create a policy to include this device group, and apply it to a particular administrator user group.

Policies

Policies define what you can do, what you can do it to, and when you can do it. Policies allow specification of days and times, port/device access, and if it was granted **control** access (Read/Write), or **deny** access (None). Policies specify a port group or device group, which defines the ports or devices a user will have access to (or not). It is important to remember that policies do not specify the user group. Therefore, you need to apply the policies to a user group.

Apply Policies to User Group

By applying a policy to a user group, you have specified which users have access to which ports and devices. The policy governs what the user group can do, what devices or ports they can access, and when they can do it. Through this process, you can implement complex administrative and security objectives.

Policy Summary

The following diagram is a visual representation of how to implement security with CC-SG:

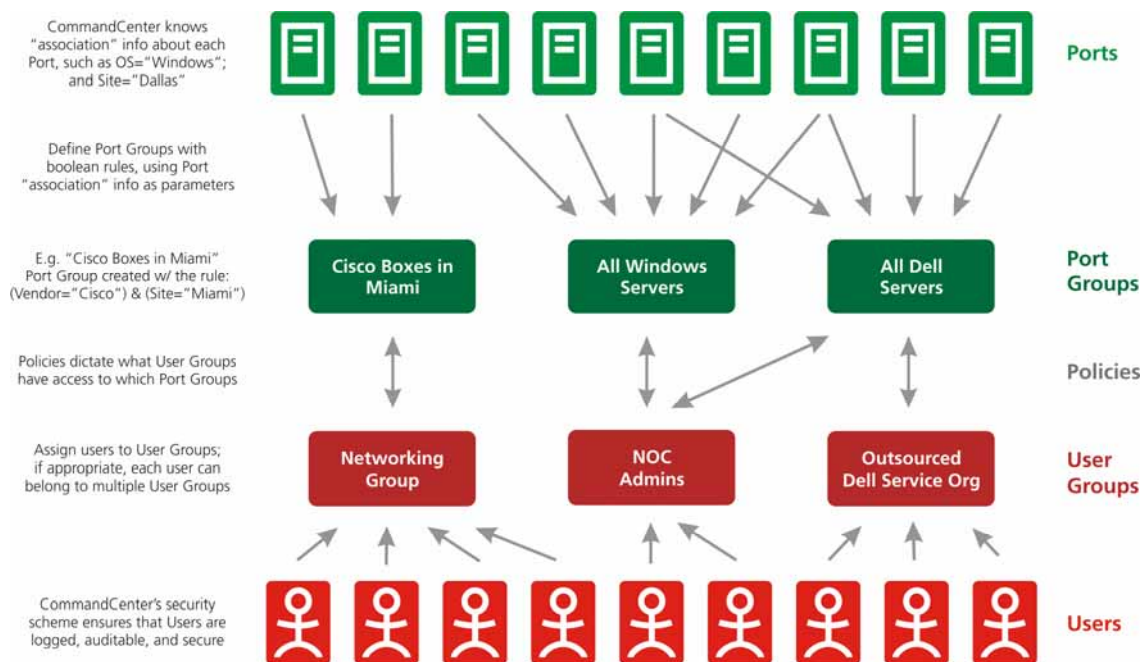


Figure 131 Ports, Port Groups, Policies, User Groups, Users

Policy Manager

Policy Manager commands allow you to add, edit, delete, and assign policies to Device and Port groups. Policies give users rights to allow or deny access to groups. Please see **Appendix C: Initial Setup Process Overview** for more information on using policies.

Add Policy

1. On the **Associations** menu, click **Policy Manager**. The **Policy Manager** screen appears.

Figure 132 Policy Manager Screen

2. Click **Add** to add a new policy. The **Add Policy** window appears.

Figure 133 Add Appliance Policy Window

3. Type the name of the new policy in the **Enter Policy Name** field.
4. Click **OK** to add the new policy or **Cancel** to close the window. If you clicked **OK**, the new policy name appears in the **Name** field.
5. Click on the **Device Group** drop-down arrow and select a device group.
6. Click on the **Port Group** drop-down arrow and select a port group.
7. Click on the up or down arrows in the **Start Time** and **End Time** fields to assign a starting time and an ending time during a 24-hour period for this policy to be in effect.
8. Select the appropriate option buttons for this policy to be in effect: **Any** to apply policy every day, **Weekday** to apply policy every working day, **Weekend** to apply policy Saturdays and Sundays, and **Custom** to manually choose the days policy to be applied. If you choose **Custom**, check on the days of the week to apply the policy.
9. Select a permission type: **Deny** or **Control**, in the **Permission** field.

10. Click **Update** to add the policy. The **Update Policy** window appears

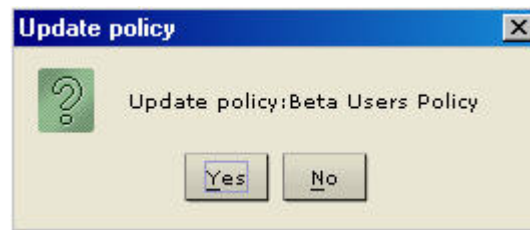


Figure 134 Update Policy Window

11. Click **Yes** to add the policy or **No** to close the window.

12. Click **Close** to close the **Policy Manager** screen.

13. Repeat steps 1 through 12 to add other policies.

Edit Policy

1. On the **Associations** menu, click **Policy Manager**. The **Policy Manager** screen appears.
2. Click on the **Name** drop-down arrow to select a policy to edit. Click **Edit** to edit the policy. The **Edit Policy** screen appears.

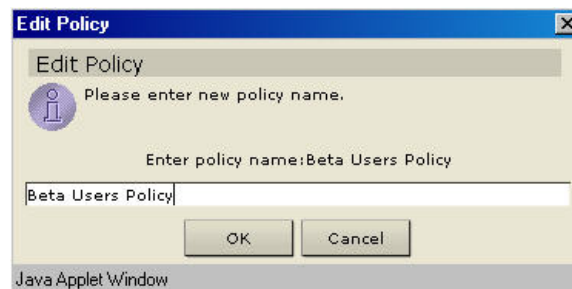


Figure 135 Edit Appliance Policy Window

3. Type a new name for the policy in the **Enter Policy Name** field.
4. Click **OK** to rename policy or **Cancel** to close the window.
5. Modify other policy elements and click **Update** to submit changes. **Update Policy** window appears.

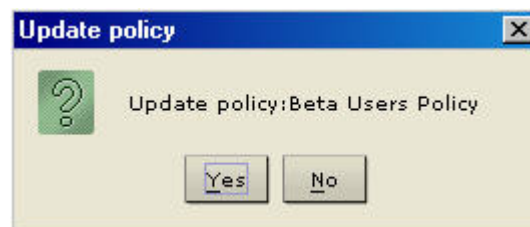


Figure 136 Update Policy Window

6. Click **Yes** to update the policy or **No** to close the window.

7. Click **Close** to close the **Policy Manager** screen.

8. Repeat steps 1 through 7 to edit other policies.

Delete Policy

1. On the **Associations** menu, click **Policy Manager**. The **Policy Manager** screen appears.
2. Click on the **Name** drop-down arrow to select a policy to be deleted. Click **Delete** to delete the policy. The **Delete Policy** window appears.

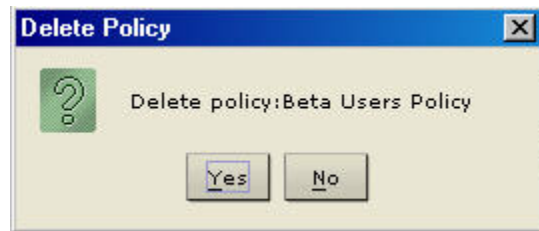


Figure 137 Delete Appliance Policy Window

3. Click **Yes** to delete the policy or **No** to close the window.
4. Click **Close** to close the **Policy Manager** screen.
5. Repeat steps 1 through 4 to delete other policies.

Note: Deleting a policy removes the policy and its association from user groups.

Chapter 9: Configuring Remote Authentication

Authentication and Authorization

Users of CC-SG can be locally authenticated and authorized on the CC-SG or remotely authenticated using the following supported directory servers:

- Microsoft Active Directory (AD)
- Netscape's Lightweight Directory Access Protocol (LDAP)
- TACACS+
- RADIUS

Any number of remote RADIUS, TACACS+, and LDAP servers can be used for external authentication. For example, you could have three Active Directory (AD) servers, two iPlanet (LDAP) servers, and three RADIUS servers.

Flow for Authentication

When remote authentication is enabled, authentication and authorization follow these steps:

1. The user logs into CC-SG with the appropriate user name and password.
2. CC-SG connects to the external server and sends the user name and password.
3. User name and password are either accepted or rejected and sent back. If authentication is rejected, this results in a failed login attempt.
4. If authentication is successful, local authorization is performed where CC-SG checks if user name entered matches a group or "users not in group" and grants privileges per the assigned policy. In the case of Active Directory authorization, the server returns a list of group names that were assigned a policy. CC-SG will then match the groups and assign the appropriate privileges as specified in the policy.

When remote authentication is disabled, both authentication and authorization are performed locally on CC-SG.

User Accounts

User Accounts must be added to the authentication server for remote authentication. Except when using Active Directory for both authentication and authorization, all remote authentication servers require that users be created on CC-SG. The user's user name on both the authentication server and on CC-SG must be the same, although the passwords may be different. The local password is used only when remote authentication is disabled. Please see **Chapter 7: Adding Users and User Groups** for additional information on adding users who will be remotely authenticated.

***Note:** If remote authentication is used, users have to contact their Administrators to change their passwords on the remote server. Passwords cannot be changed on the CC-SG server for remotely authenticated users.*

To use CC-SG for port level authorization, a local account with assigned ports must be added.

Establish Order of Authentication Databases

The General properties allow you to set the order of your authentication databases. If the first checked option is unavailable, CC-SG will try the second, then the third, and so on, until it is successful.

1. On the **Setup** menu, click **Security Manager**. When the **Security Manager** screen appears, click on the **General** tab.

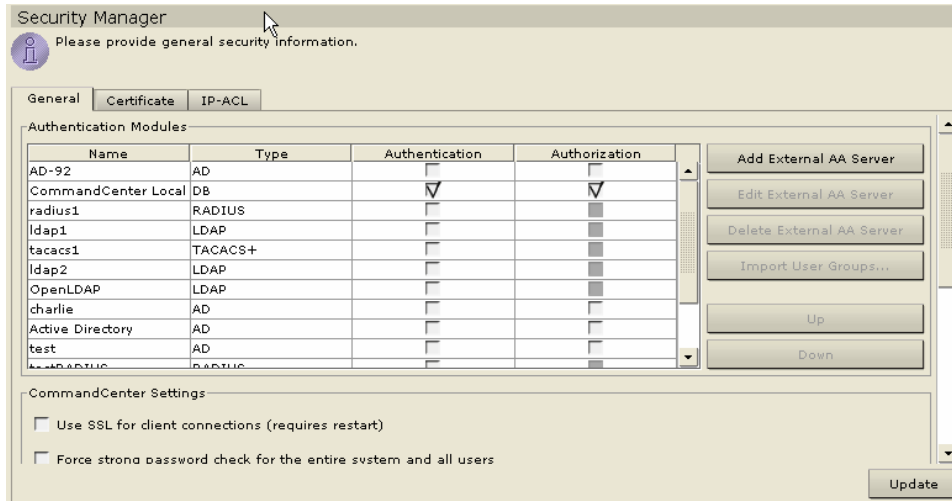


Figure 138 Security Manager General Screen

2. The modules in the table represent the multiple authentication options available in CC-SG. Select a name from the **Authentication Modules** table and click **Up** and **Down** to prioritize the sequence of engagement.
3. Check the box under the **Authentication** column to use a selected module for user authentication.
4. If the selected module is an Active Directory server or the **CC Local Database**, check the box under the **Authorization** column to use that module for user authorization as well.
5. Click **Update** to update the changes.
6. Click **Close** to close the **Security Manager** screen.

Distinguished Names for LDAP and Active Directory

Configuration of remotely authenticated users on LDAP or Active Directory servers requires entering user names and searches in Distinguished Name (DN) format. The full DN format is described in [RFC2253](#). For the purposes of this document, you need to know how to enter DNs and in what order they should be listed. For example, specifying a DN for Active Directory would be as follows:

common name (cn), organizational unit (ou), domain component (dc)

Specifying a DN for Netscape LDAP and eDirectory LDAP would be as follows:

user id (uid), organizational unit (ou), organization (o)

Username

When authenticating CC-SG users on an Active Directory server by specifying **cn=administrator,cn=users,dc=xyz,dc=com** in **username**, if a CC-SG is associated with an imported AD group, they will be granted access with these credentials. Note that you can specify more than one common name, organizational unit, and domain component.

Base DN

You also enter a Distinguished Name (DN) to specify where the search for users begins. Enter a DN in the **Base DN** field to specify an Active Directory container in which the users can be found. For example, entering: **ou=DCAdmins,ou=IT,dc=xyz,dc=com** will search all users in the **DCAdmins** and **IT** organizational units under the **xyz.com** domain.

Active Directory (AD)

Microsoft Active Directory provides a directory service that allows organizations to administer their networked resources. Active Directory is a directory server that is LDAP compliant and may be used for both authentication and authorization. If your configuration uses both, there is no need to add users to the CC-SG server since AD users are maintained independently and exclusively on the Active Directory server.

Setup on AD Server

1. On the Active Directory server, set up an account that provides credentials for CC-SG users to access the AD server. For example, you could set up a **Command Center** account in the ServiceAccounts organizational unit (ou) under the **Contuso.com** domain. This account is used to bind Active Directory to a CC-SG query.

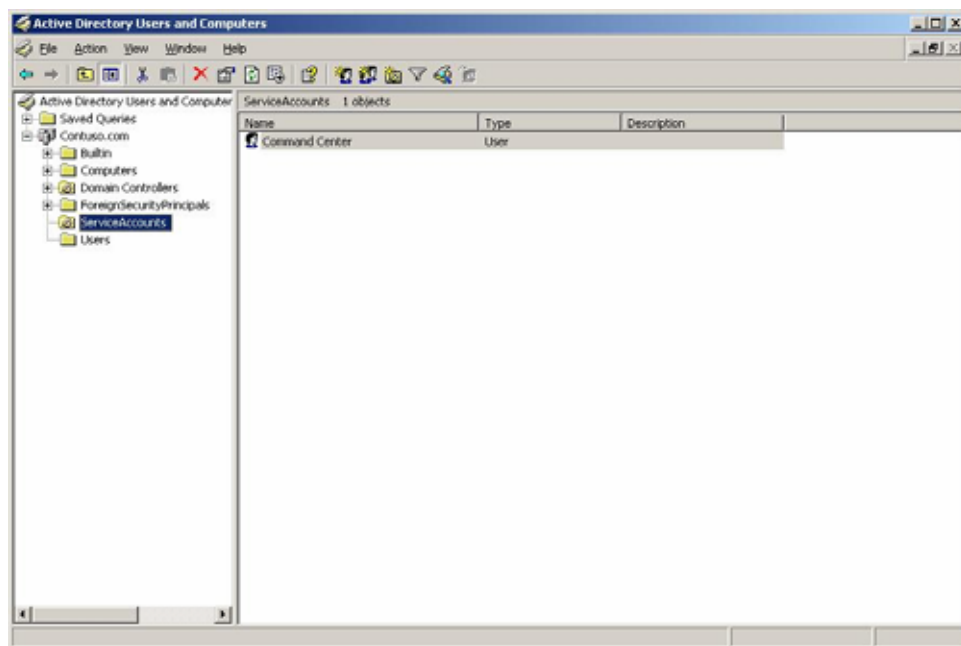


Figure 139 Active Directory Account

- On the Active Directory server, set up your users under the Users organizational unit (ou). These users will log into the CC-SG but are authenticated on the Active Directory server. Note that the display name of **joe raritan** can be different from the CC-SG login user name, for example **jraritan**.

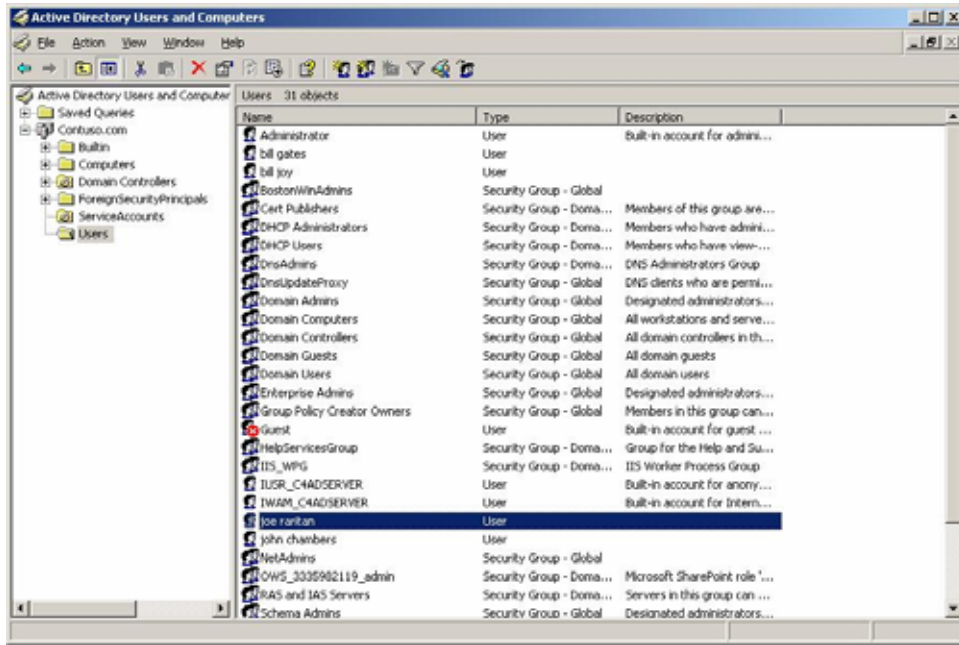


Figure 140 Active Directory Users

- On the Active Directory server, assign CC-SG users to a group, such as **CC Users**. The user group reflects the CC-SG access requirements for the users. For example, joe raritan is assigned to the CC Users group by right-clicking on the user, selecting **Properties**, and selecting CC Users in the **Member Of** tab.

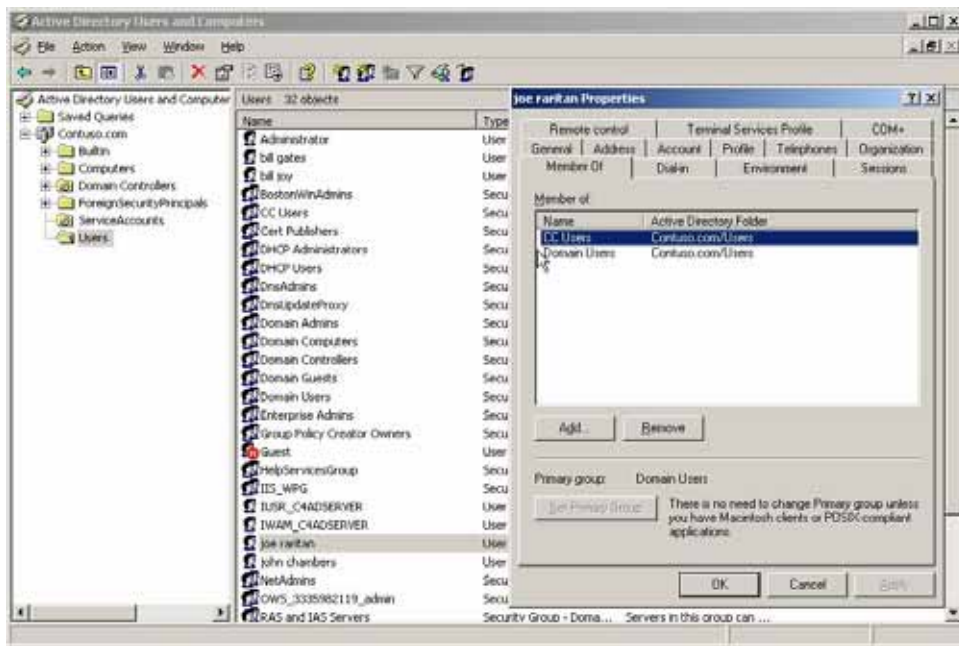


Figure 141 Assigning User to a Group

Setup on CC-SG

1. On CC-SG, click **Security Manager** from the **Setup** menu. When the **Security Manager** screen appears, click **Add External AA Server**.
2. In the **Add Module** screen, select **AD** from the **Module Type** pulldown menu.

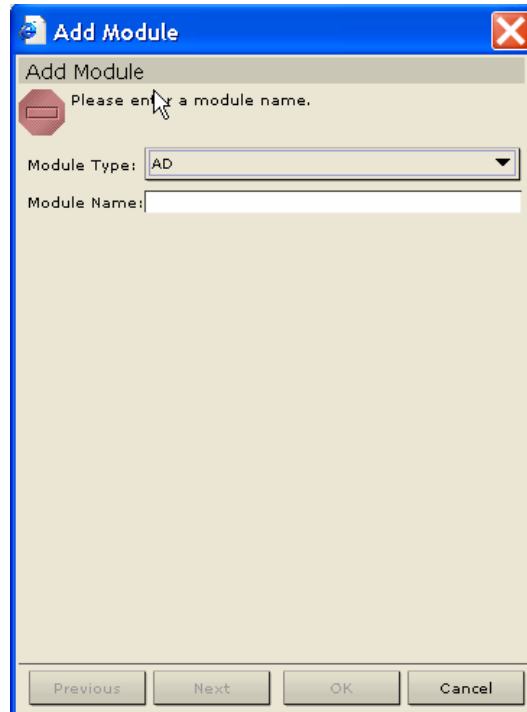


Figure 142 Specifying a Name for Active Directory Server

3. Specify a name for the Active Directory server in **Module name**. The name is optional and is specified only to distinguish this server from any others that may be configured. The name is not connected to the actual Active Directory server name in any way.
4. Click **Next**.

General Settings on CC-SG

1. Type the **IP Address/Hostname** of the Active Directory server. For hostname rules, see **Terminology/Acronyms** in **Chapter 1: Introduction**.

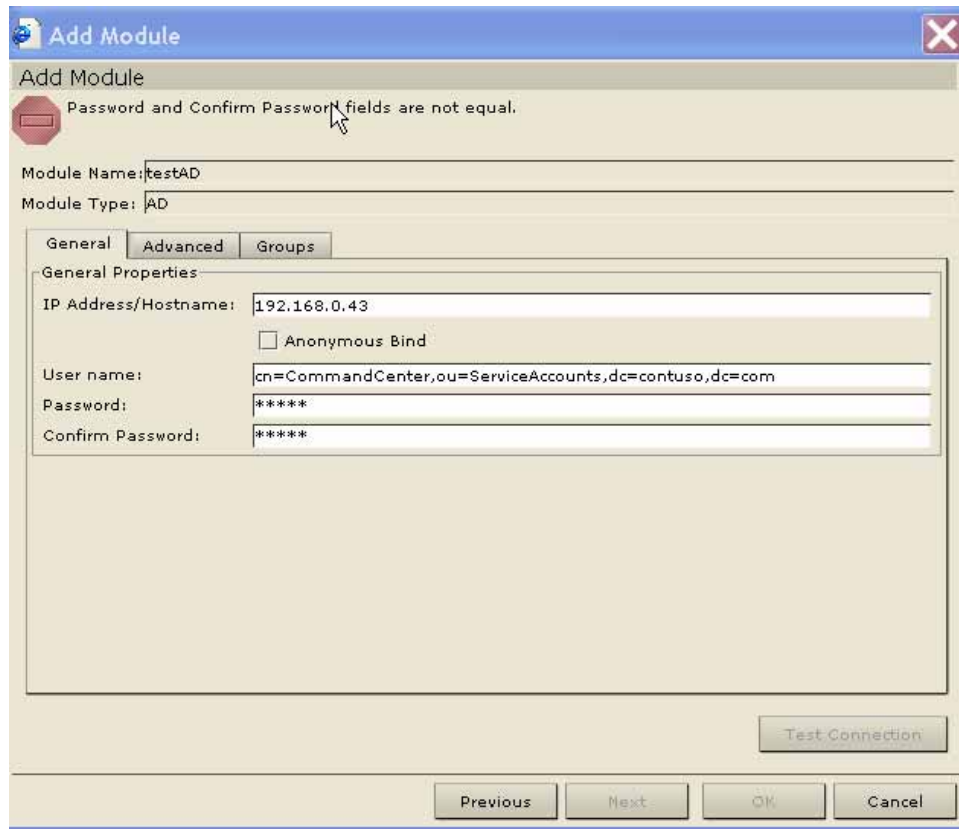


Figure 143 Specifying General Values for Active Directory Server

2. Check **Anonymous Bind** if you want to connect to the Active Directory server without specifying a username and password. If checking this option, ensure your Active Directory server allows anonymous queries.

Note: By default, Windows 2003 does NOT allow anonymous queries. Windows 2000 servers do allow certain anonymous operations, whose query results are based on the permissions of each object.

3. If not using anonymous binding, type a **User name**. The user name needs to be a valid user entry in the Active Directory directory structure and should have permissions to execute search queries. The user name can be in one of the following three forms:
 - cn=Administrator,cn=Users,dc=raritan,dc=com
 - Administrator@raritan.com
 - Administrator

Note: If using SASL to securely connect to Active Directory, use the third form (**Administrator**) for the user name.

4. Enter and confirm the **Password** for the user name if not using anonymous binding.
5. Optionally, click **Test Connection** to test the connection to the Active Directory server using the given parameters. You should receive a confirmation of a successful connection. If not, review the settings carefully for errors and try again.
6. Click **Next** to continue.

Advanced Settings on CC-SG

1. If you want to configure advanced settings, click on the **Advanced** tab.

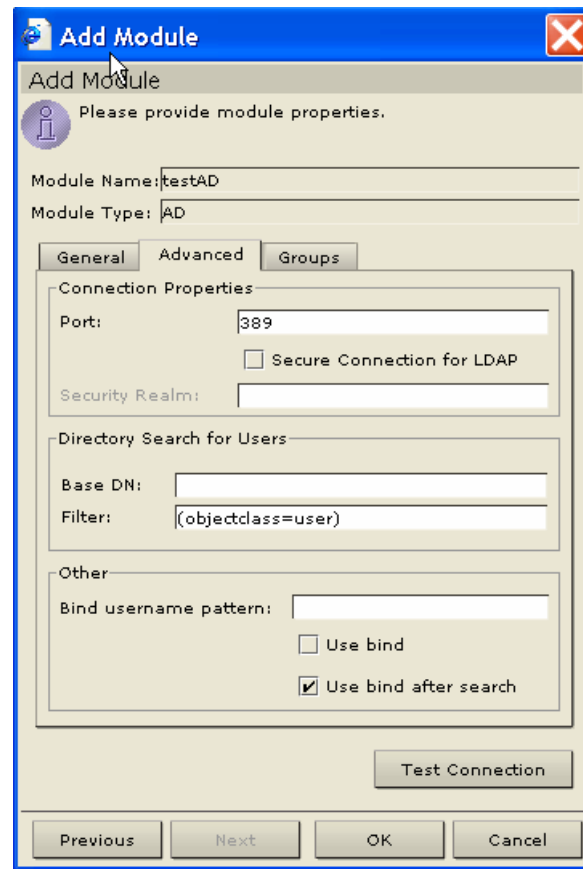


Figure 144 Specifying Advanced Values for Active Directory Server

2. Specify a port (default is **389**) on which the Active Directory server is listening.
3. Optionally, check **Secure Connection for LDAP** if you want to use a secure channel for the connection. If checked, CC-SG uses Simple Authentication and Security Layer (SASL) with Digest-MD5 authentication.
4. If using a secure connection, specify a **Security Realm** against which users will be authenticated. If using a single domain controller, it will have a single realm whose name is the same as that of the domain controller. For example, if the Domain Controller is `dc=raritan,dc=com`, then the default realm will be **raritan.com**. If a realm is not specified, the default will be used or one will be selected for you if there are multiple realms.

Note: You may have multiple AD servers connected in a trusted forest. Each AD server will have a separate security realm. For example, you may have AD1 and AD2 with security realms of **realm_AD1** and **realm_AD2** respectively. If a connection is made to AD1 but you want to authenticate a user in AD2, you need to inform AD1 the realm of the user (**realm_AD2**) to correctly redirect the authentication request. In this case, you need to configure CC-SG to connect to AD1 and specify **realm_AD2** to authenticate users against AD2.

5. Specify a **Base DN** (directory level/entry) under which the authentication search query will be executed.

EXAMPLE	DESCRIPTION
dc=raritan,dc=com	The search query for the user entry will be made over the whole directory structure.
cn=Administrators,cn=Users,dc=raritan,dc=com	The search query for the user entry will be performed only in the Administrators sub-directory (entry).

6. Type a user's attributes in **Filter** so the search query will be restricted to only those entries that meet this criterion. By default, the filter is **objectclass=user** which means that only entries of type **user** are searched.
7. Specify the way in which the search query will be performed for the user entry. If you check **Use Bind**, CC-SG attempts to connect (bind) to AD directly with the username and password supplied in the applet. However, if a username pattern is specified in **Bind username pattern**, the pattern will be merged with the username supplied in the applet and the merged username will be used to connect to the AD server.
*For example, if you have **cn={0},cn=Users,dc=raritan,dc=com** and **TestUser** has been supplied in the applet, then CC-SG uses **cn=TestUser,cn=Users,dc=raritan,dc=com** to connect to the AD server. Only check **Use Bind** when the user logging in from the applet has permissions to perform search queries in the AD server.*
8. Check **Use Bind After Search** to use the username and password specified in the **General** tab to connect to the AD server. The entry is searched in the specified Base DN and is found if it meets the specified filtering criterion and if the attribute "samAccountName" is equal to the username entered in the applet. Then a second connection (bind) is attempted using the username and password supplied in the applet. This second bind assures that the user provided the correct password.

Group Settings on CC-SG

Use to retrieve groups from the AD server and import into CC-SG local database for authorization purposes.

1. Click on the **Groups** tab.

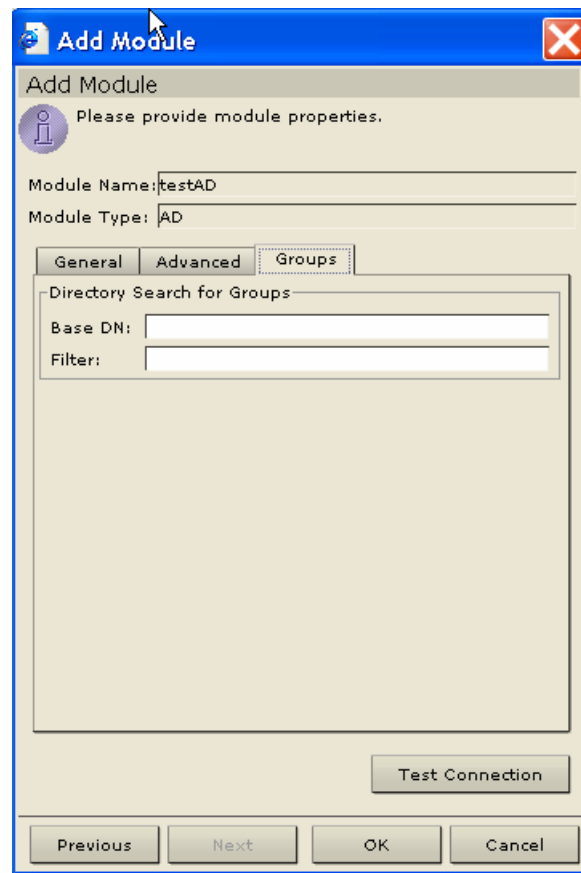


Figure 145 Specifying Group Values for Active Directory Server

2. Specify a **Base DN** (directory level/entry) under which the groups, containing the user to be authorized, will be searched.

EXAMPLE	DESCRIPTION
dc=raritan,dc=com	The search query for the user in the group will be made over the whole directory structure.
cn=Administrators,cn=Users,dc=raritan,dc=com	The search query for the user in the group will be performed only in the Administrators sub-directory (entry).

3. Type a user's attributes in **Filter** so the search query for the user in the group will be restricted to only those entries that meet this criterion. For example, if you specify **cn=Groups,dc=raritan,dc=com** as the Base DN and **(objectclass=group)** as the Filter, then all entries that are in the **Groups** entry and are of type **group** will be returned.
4. Click **OK** to save the settings.

- On CC-SG, in the **Security Manager** screen, click **Import Groups...** to retrieve a list of user group values stored on the Active Directory server. If any of the user groups are not already on the CC-SG, you can import them here and assign them an access policy.



Figure 146 Importing Groups from Active Directory Server

- Check the boxes next to the groups you wish to import to CC-SG, such as CC Users.

Note: To save time in searching and finding the groups you want to import, you can manually add the user groups in CC-SG instead as long as the name and case of the user group is the same—see **Chapter 7: Adding Users and User Groups** for details. Then assign the user group an access policy.

- In the Policies column, assign those groups to a CC-SG access policy. These policies should already be created, please see **Chapter 8: Creating Policies** for details on adding policies.
- Click **Import** to import the selected user groups.
- To check that the group was imported properly and to view the privileges of the group just imported, click on the **Users** tab, right-click on the group, and select **Edit User Group**.

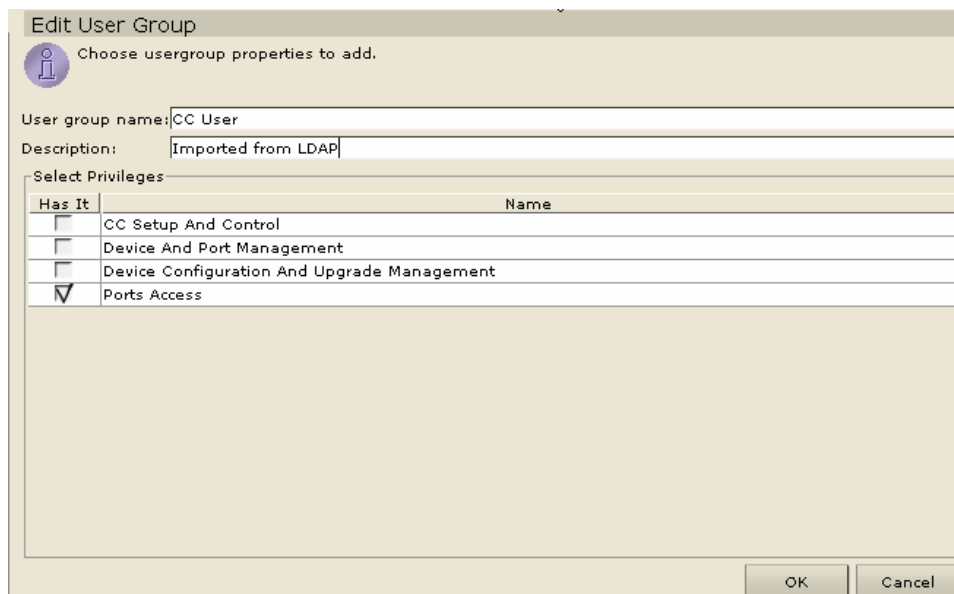


Figure 147 Viewing Privileges of Imported Group

10. Verify the policy of the group that was imported by clicking the **Users** tab, right-clicking on the group and selecting **Edit User Group Policies**. Look under **Selected Policies** to confirm the policy that the correct policy was assigned to the group.

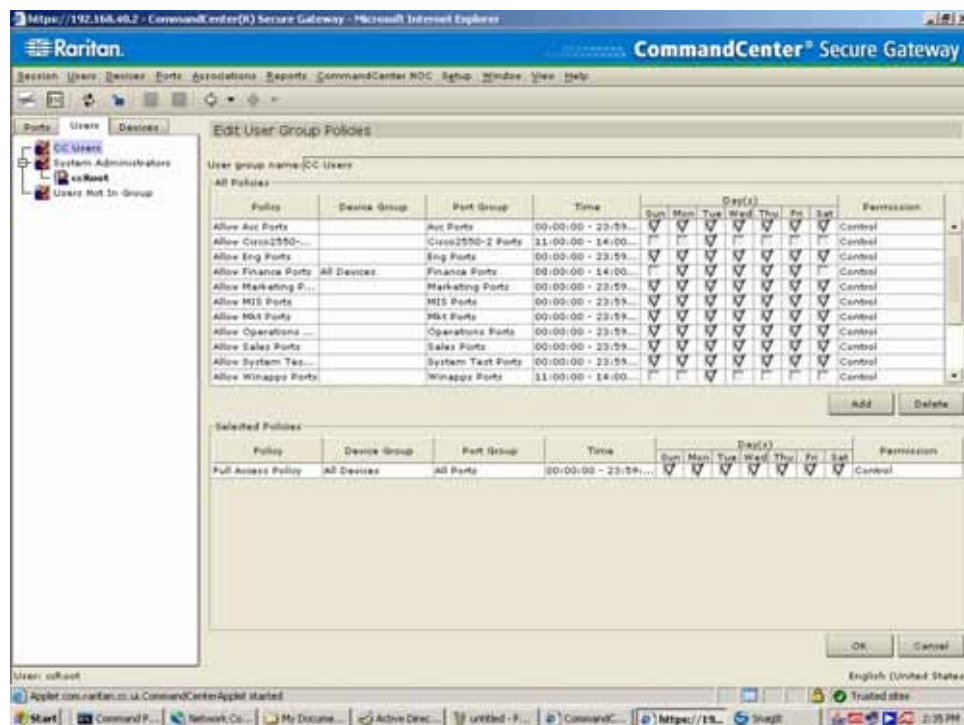


Figure 148 Viewing Policy of Imported Group

11. When the user, such as **jraritan**, logs in, they will be authenticated by the Active Directory server and the login appears at the bottom of the window, for example **jraritan@ldap1**.

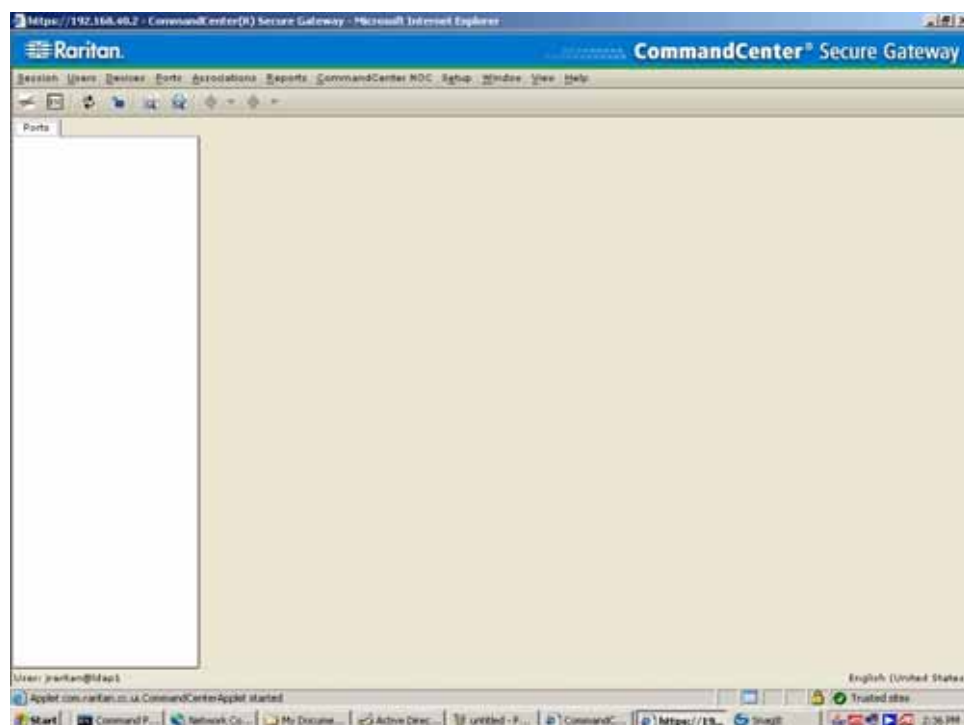


Figure 149 Logging In as Remotely Authenticated User

LDAP (Netscape)

Once the CC-SG applet is started and a user name and password are entered, a query is forwarded either through CC-SG or directly to the LDAP server. If the username and password match those in the LDAP directory, the user is authenticated. The user will then be authorized against the local user groups on the LDAP server.

1. On the **Setup** menu, click **Security Manager**. When the **Security Manager** screen appears, click **Add External AA Server** in the **General** tab.

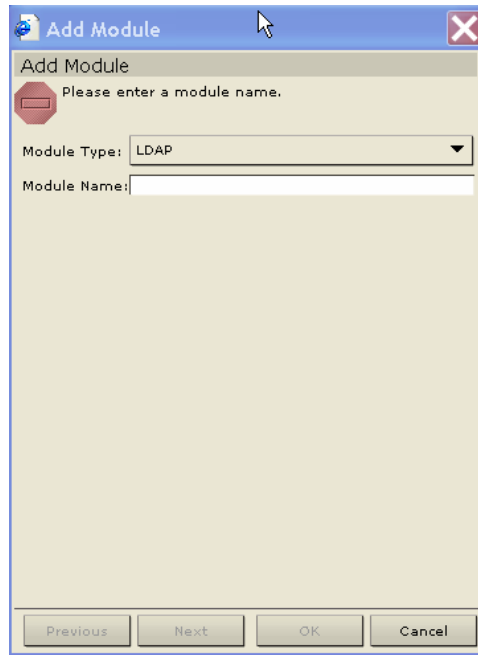


Figure 150 Security Manager Add Module Screen

2. In **Add Module** screen, select **LDAP** from the pulldown menu, specify a name for the server, and click **Next**.

Figure 151 Security Manager LDAP Screen General Tab

3. Type the IP address or hostname of the LDAP server in the **IP Address/Hostname** field. For hostname rules, see **Terminology/Acronyms** in **Chapter 1: Introduction**.
4. Type the port value in the **Port** field. The default port is 389.
5. Check **Secure Connection for LDAP** if using a secure LDAP server and enter a security realm.
6. Check **Anonymous Bind** if your LDAP server allows anonymous queries. You do not need to enter a user name and password with anonymous binding.

Note: By default, Windows 2003 does NOT allow anonymous queries. Windows 2000 servers do allow certain anonymous operations, whose query results are based on the permissions of each object.

7. If not using anonymous binding, type a **User name** and **Password**. Enter a Distinguished Name (DN) to specify the credentials used to query the AD server. For DN, enter the common name, organizational unit, and domain. For example, type **uid=admin,ou=Administrators,ou=TopologyManagement,o=NetscapeRoot**. Separate the values with commas but do not use spaces before or after the comma. The value themselves can include spaces, such as **Command Center**.
8. Enter and confirm the password.
9. To specify where the search for users begins, enter a Distinguished Name in **Base DN**. For example, **ou=Administrators,ou=TopologyManagement,o=NetscapeRoot**, searches all organizational units under the domain.
10. To narrow searching to only particular types of objects, enter a value in **Filter**. For example, **(objectclass=person)** will narrow searching to only person objects.

11. Click **Test Connection** to test the LDAP server using the given parameters. You should receive a confirmation of a successful connection. If not, review the settings carefully for errors and try again.
12. Click on the **Advanced** tab to set advanced configuration options for the LDAP server.

Figure 152 Security Manager LDAP Screen Advanced Tab

13. Click the radio button for **Base 64** or **Plain Text** depending on whether you want the password to be sent to the LDAP server with encryption or as plain text.
14. Click on the **Default Digest** drop-down arrow and select the default encryption of user passwords.
15. Type the user attribute and group membership attribute parameters in the **User Attribute** and **Group Membership Attribute** fields. These values should be obtained from your LDAP directory schema.
16. Type the bind pattern in the **Bind Username Pattern** field.
17. Check **Use Bind** if you want CC-SG to send the username and password entered at login to the LDAP server for authentication. If **Use Bind** is *not checked*, CC-SG will search the LDAP server for the user name, and if found, will retrieve the LDAP object and locally compare the associated password with the one entered.
18. On some LDAP servers, the password cannot be retrieved as part of the LDAP object. Check **Use Bind After Search** to instruct CC-SG to bind the password to the LDAP object again and send it back to the server for authentication.
19. Click **OK**.

Sun One LDAP (iPlanet) Configuration Settings

If using a Sun One LDAP server for remote authentication, use this example for parameter settings:

PARAMETER NAME	SUN ONE LDAP PARAMETERS
IP Address/Hostname	<Directory Server IP Address>
User Name	CN=<Valid user id>
Password	<Password>
BaseDN	O=<Organization>
Filter	(objectclass=person)
Passwords (Advanced Screen)	Plain Text
Password Default Digest (Advanced)	SHA
Use Bind	unchecked
Use Bind After Search	Checked

OpenLDAP (eDirectory) Configuration Settings

If using an OpenLDAP server for remote authentication, use this example:

PARAMETER NAME	OPEN LDAP PARAMETERS
IP Address/Hostname	<Directory Server IP Address>
User Name	CN=<Valid user id>, O=<Organization>
Password	<Password>
User Base	O=accounts, O=<Organization>
User Filter	(objectclass=person)
Passwords (Advanced screen)	Base64
Password Default Digest (Advanced)	Crypt
Use Bind	Unchecked
Use Bind After Search	Checked

TACACS+

CC-SG users who are remotely authenticated by a TACACS+ server need to be created on the TACACS+ server and on CC-SG. The user's user name on the TACACS+ server and on CC-SG must be the same, although the passwords may be different. Please see **Chapter 7: Adding Users and User Groups** for additional information on adding users who will be remotely authenticated.

1. On the **Setup** menu, click **Security Manager**. When the **Security Manager** screen appears, click **Add External AA Server** in the **General** tab.

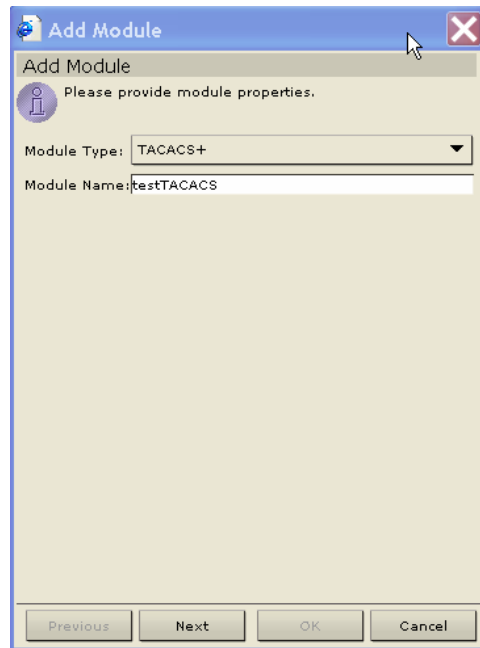


Figure 153 Security Manager Add Module Screen

2. In the **Add Module** screen, select **TACACS+** from the pulldown menu, specify a name for the server, and click **Next**.



Add Module

Add Module

Please provide module properties.

Module Name: test

Module Type: TACACS+

IP Address/Hostname: localhost

Port number: 49

Authentication port: tty01

Shared key: *****

Shared key confirm: *****

Previous Next OK Cancel

Figure 154 Specifying a TACACS+ Server

3. Type the IP address or hostname of the TACACS+ server in the **IP Address/Hostname Name** field. For hostname rules, see **Terminology/Acronyms** in **Chapter 1: Introduction**.
4. Type the port number in the **Port Number** field.
5. Type the authentication port in the **Authentication Port** field.
6. Type and confirm the shared key into the **Shared Key** field.
7. Click **OK** to update changes.

RADIUS

CC-SG users who are remotely authenticated by a RADIUS server need to be created on the RADIUS server and on CC-SG. The user's user name on the RADIUS server and on CC-SG must be the same, although the passwords may be different. Please see **Chapter 7: Adding Users and User Groups** for additional information on adding users who will be remotely authenticated.

1. On the **Setup** menu, click **Security Manager**. When the **Security Manager** screen appears, click **Add External AA Server** in the **General** tab.

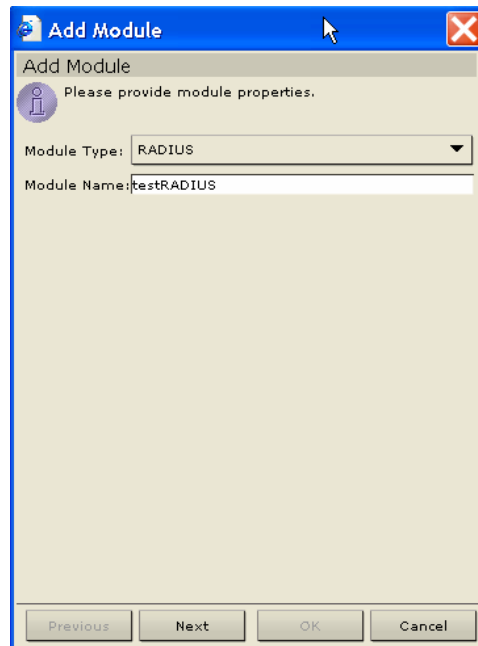


Figure 155 Security Manager Add Module Screen

2. In **Add Module** screen, select **RADIUS** from the pulldown menu, specify a name for the server, and click **Next**.

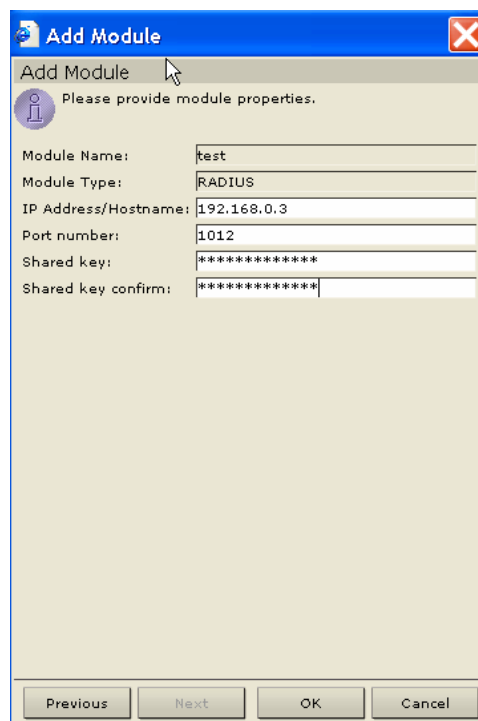


Figure 156 Specifying a RADIUS Server

3. Type the IP address or hostname of the RADIUS server in the **IP Address/Hostname** field. For hostname rules, see **Terminology/Acronyms** in **Chapter 1: Introduction**.
4. Type the port number in the **Port Number** field.
5. Type and confirm the shared key into the **Shared Key** field.
6. Click **OK** to update changes.

Certificate

Options in this window can be used to generate a certificate signing request (also CSR or certification request). A CSR is a message sent from an applicant to a certificate authority to apply for a digital identity certificate. Before creating a CSR, the applicant first generates a key pair, keeping the private key secret. The CSR contains information identifying the applicant (such as a directory name in the case of an X.509 certificate), and the public key chosen by the applicant.

1. On the **Setup** menu, click **Security Manager**.
2. When the **Security Manager** screen appears, click on the **Certificate** tab.

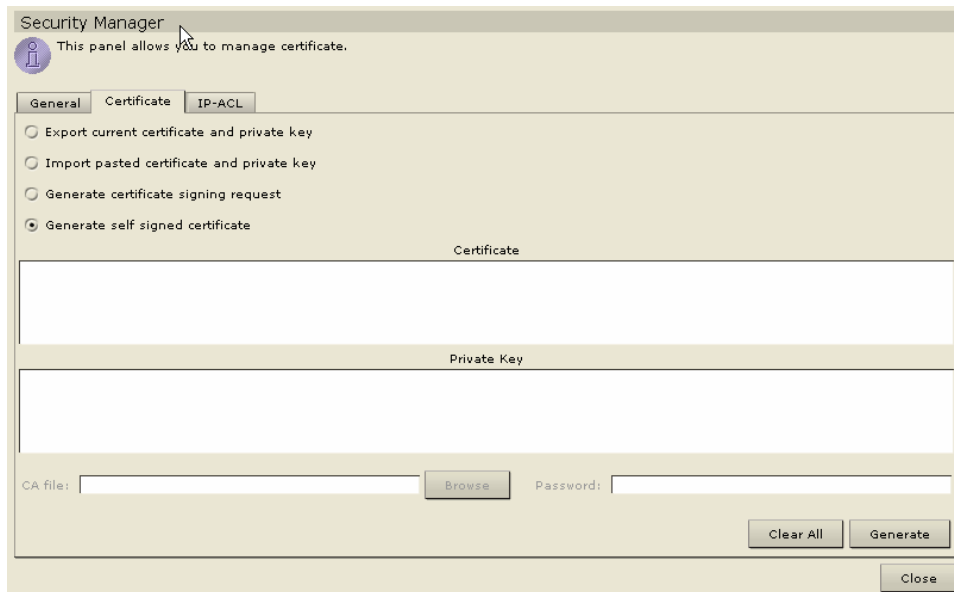


Figure 157 Security Manager Certificate Screen

Export Current Certificate and Private Key

Click **Export Current Certificate and Private Key**. The certificate appears in the **Certificate** panel and the private key appears in **Private Key** panel. Copy the text of the **Certificate** and **Private Key** and submit it by clicking **Export**.

Generate Certificate Signing Request

The following explains how to generate a CSR and a private key on CC-SG. The CSR will be submitted to the Certificate Server who will issue a signed certificate. A root certificate will also be exported from the Certificate Server and saved in a file. The signed certificate, root certificate, and private key will then be imported.

1. Click **Generate Certificate Signing Request** and click **Generate**. The **Generate Certificate Signing Request** window appears.
2. Type the requested data for the CSR into the fields.

Figure 158 Generate Certificate Signing Request Screen

3. Click **OK** to generate the CSR or **Cancel** to exit the window. The CSR and Private key appears in the corresponding fields of the **Certificate** screen.

Figure 159 Certificate Request Generated

4. Using an ASCII editor, for example, Notepad, copy and paste the CSR into a file and save it with a **.cer** extension.
5. Using an ASCII editor, for example, Notepad, copy and paste the Private Key into a file and save it as a text file.
6. Submit the CSR file (**.cer**) saved in Step 4. to the Certificate Server to obtain a signed certificate from the Server.
7. Download or export the root certificate from the Certificate Server and save it to a file with a **.cer** extension. This is a different certificate from the signed certificate that will be issued by the Certificate Server in the next step.
8. Once you receive the signed certificate from the Certificate Server, click **Import pasted certificate and private key**.
9. Copy and paste the signed certificate into the Certificate Request field. Paste the Private Key that was saved previously into the Private Key field.
10. Click **Browse** next to **CA file:** and select the root certificate file that was saved in Step 6.

11. Type **raritan** in the **Password** field if the CSR was generated by CC-SG. If a different application generated the CSR, use that password for that application.

Note: If the imported certificate is signed by a root and subroot CA (certificate authority), using only a root or subroot certificate will fail. To resolve this, copy and paste both root and subroot certificate into one file and then import it.

Generate Self Signed Certificate Request

Click on the **Generate Self Signed Certificate** option button and click **Generate**. The **Generate Self Signed Certificate** window appears. Type the data needed for the self-signed Certificate into the fields. Click **OK** to generate the certificate or **Cancel** to exit the window. The Certificate and Private Key will appear encrypted in the corresponding fields of the **Certificate** screen.



Figure 160 Generate Self Signed Certificate Window

IP-ACL

This feature restricts access to CC-SG based on IP addresses. Specify an IP-access control list (IP-ACL) by entering an IP address range, the group to which it applies, and an Allow/Deny privilege.

1. On the **Setup** menu, click **Security Manager**. When the **Security Manager** screen appears, click on the **IP-ACL** tab.

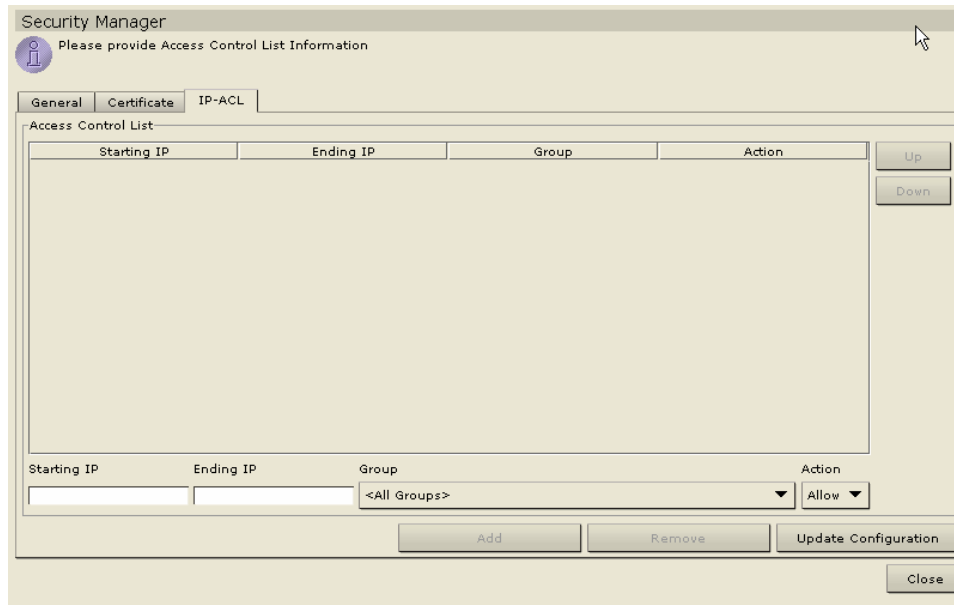


Figure 161 Security Manager IP-ACL Screen

2. To change the order of the line items in the **Access Control List**, select the line item and click **Up** or **Down**. Connecting users will be allowed or denied according to the first rule that applies (from top to bottom).
3. To add a new item to the list, specify a range to apply the rule to by typing the starting IP value in the **Starting IP** field, and the ending IP value in the **Ending IP** field.
4. Click on the **Group** drop-down arrow to select a group to apply the rule to.
5. Click on the **Action** drop-down arrow and choose to **Allow** or **Deny** the group access to the IP range.
6. Click **Add** to add the new rule to the **Access Control List**.
7. To remove any line item, select it and click **Remove**.
8. Click **Update Configuration** to update your system with the new access control rules.

Chapter 10: Generating Reports

Reports can be sorted by clicking on the column headers. Click on a column header such as User Name, Access Time, etc., to sort report data by that value. The data will refresh in ascending order alphabetically, numerically, or chronologically. Click on the column header again to sort in descending order. Please note the arrowhead pointing upwards or down next to the cell name, indicating how the report is sorted.

The column width in all reports can be sized by resting your mouse pointer on the column divider in the header row until it becomes a double-headed arrow. Click and drag the arrow to the left or right to adjust column width.

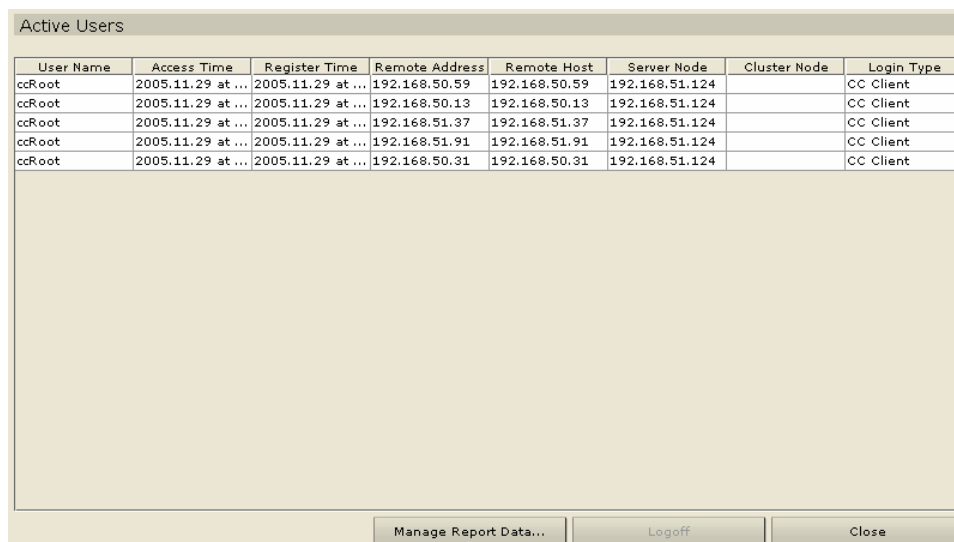
The sorting value and column width you use becomes the default report view the next time you log in and run CC-SG reports. For all reports, you can double-click on a row to view further details of the report.

*Note: In all reports, use **CTL+click** to deselect a highlighted row.*

Active Users Report

The Active Users report displays current users and user sessions. You can view users and disconnect them from this report.

1. On the **Reports** menu, click **Active Users**. The **Active Users** report is generated.

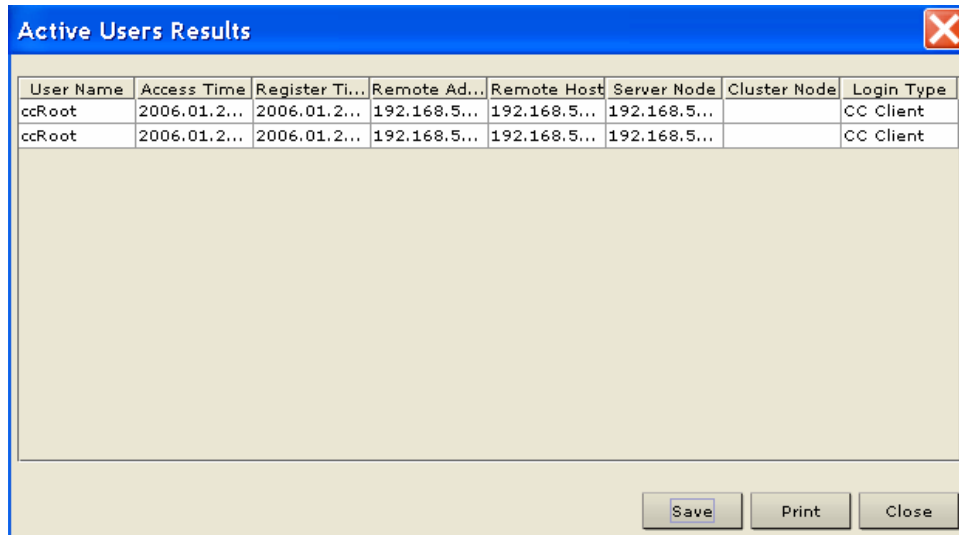


User Name	Access Time	Register Time	Remote Address	Remote Host	Server Node	Cluster Node	Login Type
ccRoot	2005.11.29 at ...	2005.11.29 at ...	192.168.50.59	192.168.50.59	192.168.51.124		CC Client
ccRoot	2005.11.29 at ...	2005.11.29 at ...	192.168.50.13	192.168.50.13	192.168.51.124		CC Client
ccRoot	2005.11.29 at ...	2005.11.29 at ...	192.168.51.37	192.168.51.37	192.168.51.124		CC Client
ccRoot	2005.11.29 at ...	2005.11.29 at ...	192.168.51.91	192.168.51.91	192.168.51.124		CC Client
ccRoot	2005.11.29 at ...	2005.11.29 at ...	192.168.50.31	192.168.50.31	192.168.51.124		CC Client

Figure 162 Active Users Report

2. To disconnect user, select the user name to be disconnected and click **Logoff** to disconnect the selected users from their current sessions.

- Click **Manage Report Data...** to save or print the report. Click **Save** to save the report to a location of your choice or **Print** to print the report.



User Name	Access Time	Register Ti...	Remote Ad...	Remote Host	Server Node	Cluster Node	Login Type
ccRoot	2006.01.2...	2006.01.2...	192.168.5...	192.168.5...	192.168.5...		CC Client
ccRoot	2006.01.2...	2006.01.2...	192.168.5...	192.168.5...	192.168.5...		CC Client

Buttons: Save, Print, Close

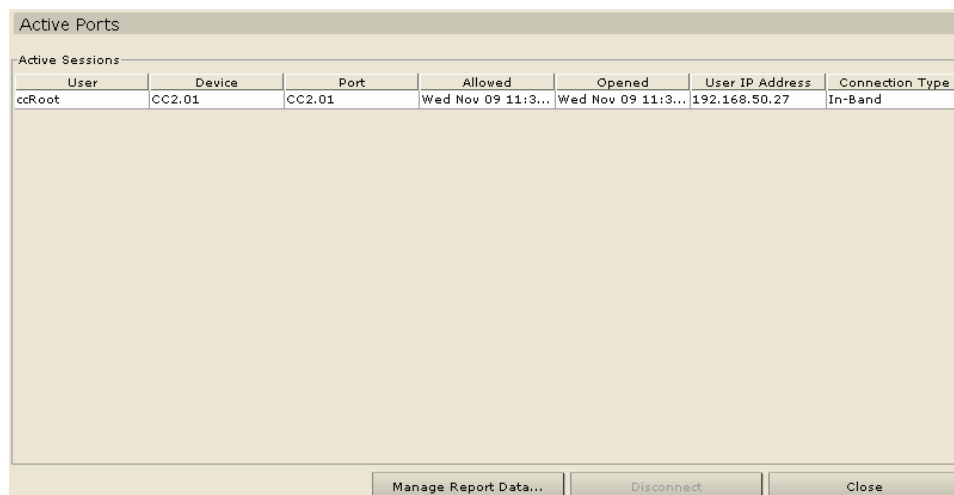
Figure 163 Manage Report Window

- Click **Close** to close the **Manage Report** window.
- Click **Close** to close the **Active Users** report.

Active Ports Report

The Active Ports report displays ports that are currently in use. You can view or disconnect ports from this report.

- On the **Reports** menu, click **Active Ports**. The **Active Ports** report is generated.



User	Device	Port	Allowed	Opened	User IP Address	Connection Type
ccRoot	CC2.01	CC2.01	Wed Nov 09 11:3...	Wed Nov 09 11:3...	192.168.50.27	In-Band

Buttons: Manage Report Data..., Disconnect, Close

Figure 164 Active Ports Report

- To disconnect a port, select the port to be disconnected and click **Disconnect** to disconnect the selected ports from their current sessions.
- Click **Manage Report Data** to save or print the report. Click **Save** to save the report to a location of your choice or **Print** to print the report. Click **Close** to close the window.
- Click **Close** to close the **Active Ports** report.

Asset Management Report

The **Asset Management** report displays data on current devices.

1. On the **Reports** menu click **Asset Management Report**. The **Asset Management** report is generated.

Name	Description	Type	IP Address	TCP Port	Version
AD-92		Generic Device	192.168.51.92		
BianorTestDevice	testing TargetMana...	Generic Device	127.0.0.1		
BianorWSTestDevice		Generic Device	10.0.1.180		
CC-124		Generic Device	192.168.51.124		
CC-52-175		Generic Device	192.168.52.175		
Dominion-KX	Dominion KX model ...	Dominion KX	192.168.51.200	5000	1.4.0.1.5
Gayle's Laptop	Gayle's Laptop	Generic Device	192.168.50.218		
IPMI-22	IPMI Server ver. 1.5	IPMI Server	192.168.51.22		
KSX223		Dominion KSX	192.168.51.223	5000	3.21.9
PC-111		Generic Device	192.168.51.111		
PC-112		Generic Device	192.168.51.112		
PC17		Generic Device	192.168.51.17		
SX-229		Dominion SX	192.168.51.229	5000	2.5.6.2
Win XP	WinXP	Generic Device	192.168.53.133		
aPS8		PowerStrip			
iLO-40-21		iLO/RILO	192.168.40.21	80	
iLO-52-108		iLO/RILO	192.168.52.108	80	1.82

Figure 165 Asset Management Report

2. Click on the **Device Type** drop-down arrow to display a list of possible devices for which to run the report. Select one and click **Apply** to run the report.
3. Press **Refresh** to update the query and generate a new report. Please note that the report may take several minutes, based on the size of your system configuration.
4. Click **Manage Report Data...** to save or print the report. Click **OK** to save the report to a location of your choice or **Print** to print the report. Click **Close** to close the window.
5. Click **Close** to close the **Asset Management** report.

Note: The **Version** column will be marked in red for a device if that device's version does not satisfy the **Compatibility Matrix**.

Audit Trail Report

The **Audit Trail** report displays audit logs and access in CC-SG. It captures actions such as adding, editing, or deleting devices or ports, and other modifications.

CC-SG maintains an Audit Trail of the following events:

- When CC-SG is launched
- When CC-SG is stopped
- When a user logs on CC-SG
- When a user logs off CC-SG
- When a user starts a port connection

1. On the **Reports** menu, click **Audit Trail**. The **Audit Trail** screen appears.

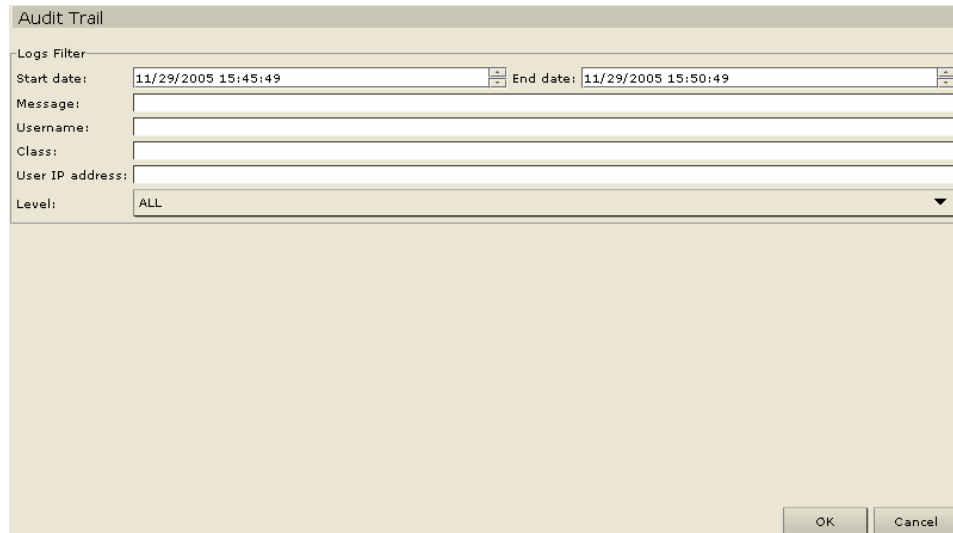


Figure 166 Audit Trail Screen

2. Select the date range for the report by either typing the date and time in the **Start Date** and **End Date** fields using the format **yyyy/mm/dd hh:mm:ss**, or by using the <→> key on your keyboard to advance through the sections and click on the up/down arrows to build the date and time.
3. Type the criteria with which to filter the report in the **Message**, **User Name**, **Class**, or **User IP Address** fields.
4. Click on the **Level** drop-down arrow to select a tracing level for the report.
5. Click **OK** to run the report.

Note: Leave some or all fields blank, depending on information desired. Leaving all fields blank retrieves the audit trail for the entire system.

6. The Audit Trail report is generated, displaying data about sessions that occurred during the designated time period.

Audit Trail							Previous
No.	Date	User	User IP Ad...	Class	Level	Message	
301	2006.01.1...			com.rarita...	INFO	User ccRoo...	Next
302	2006.01.1...	ccRoot	192.168.5...	com.rarita...	INFO	User ccRoo...	
303	2006.01.1...		192.168.5...	com.rarita...	INFO	User ccRoo...	
304	2006.01.1...		192.168.5...	com.rarita...	INFO	User ccRoo...	
305	2006.01.1...			com.rarita...	INFO	User ccRoo...	
306	2006.01.1...			com.rarita...	INFO	User ccRoo...	
307	2006.01.1...	ccRoot	192.168.5...	com.rarita...	INFO	Appliance ...	
308	2006.01.1...	ccRoot	192.168.5...	com.rarita...	INFO	Appliance ...	
309	2006.01.1...	ccRoot	192.168.5...	com.rarita...	WARN	java.net.S...	
310	2006.01.1...	ccRoot	192.168.5...	com.rarita...	INFO	Added app...	
311	2006.01.1...	ccRoot	192.168.5...	com.rarita...	INFO	Added app...	
312	2006.01.1...			com.rarita...	WARN	intercept:E...	
313	2006.01.1...	ccRoot	192.168.5...	com.rarita...	WARN	execute:e...	
314	2006.01.1...	ccRoot	192.168.5...	com.rarita...	WARN		
315	2006.01.1...	ccRoot	192.168.5...	com.rarita...	INFO	Appliance ...	
316	2006.01.1...	ccRoot	192.168.5...	com.rarita...	INFO	execute: A...	
317	2006.01.1...	ccRoot	192.168.5...	com.rarita...	WARN	execute:e...	
318	2006.01.1...	ccRoot	192.168.5...	com.rarita...	INFO	Audit Trail ...	
319	2006.01.1...	ccRoot	192.168.5...	com.rarita...	INFO	Audit Trail ...	
320	2006.01.1...	ccRoot	192.168.5...	com.rarita...	INFO	Audit Trail ...	
321	2006.01.1...						
Manage Report Data...							Clear
							Close

Figure 167 Audit Trail Report

7. Click **Manage Report Data...** to save or print the report. Click **Save** to save the records that are displayed to a CSV file or click **Save All** to save all records. Click **Print** to print the records that are displayed or **Print All** to print all records. Click **Close** to close the window.
8. Click **Clear** to clear the contents of the report.
9. If the report is lengthy, click **Next** or **Previous** to navigate through the pages.
10. Click **Close** to close the **Audit Trail** report.

Error Log Report

CC-SG stores error messages in a series of Error Log files, which can be brought up and used to help troubleshoot system problems.

You can filter the search criteria by date, message type, username, class, host, and level. Messages can be grouped by fatal, error and warning level. Once filters are selected, you can view the report results and take precautionary actions.

1. On the **Reports** menu, click **Error Log**. The **Error Log** screen appears.

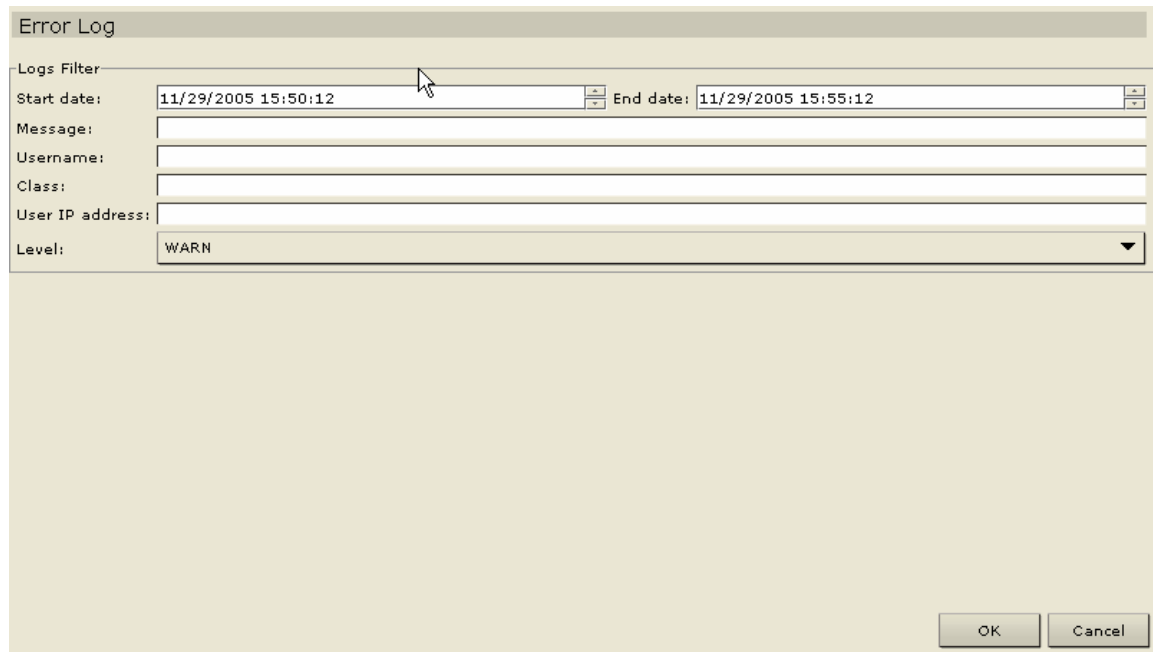
The screenshot shows a web-based interface titled "Error Log". Below the title is a "Logs Filter" section containing several input fields: "Start date:" with the value "11/29/2005 15:50:12", "End date:" with the value "11/29/2005 15:55:12", "Message:", "Username:", "Class:", "User IP address:", and "Level:" with a dropdown menu currently showing "WARN". At the bottom right of the form are "OK" and "Cancel" buttons. The background of the interface is a light beige color.

Figure 168 Error Log Screen

2. Select the date range for the report by either typing the date and time in the **Start Date** and **End Date** fields using the format **yyyy/mm/dd hh:mm:ss**, or by using the <→> key on your keyboard to advance through the sections and click on the up/down arrows to build the date and time.
3. Type the criteria with which to filter the report in the **Message**, **User Name**, **Class**, or **User IP address** fields.
4. Click on the **Level** drop-down arrow to select a tracing level for the report.
5. Click **OK** to run the report.

Note: Leave some or all fields blank, depending on information desired. Leaving all fields blank retrieves the logs for the entire system.

- The Error Log report is generated, displaying data about sessions that occurred during the designated time period.

Error Log						
No.	Date	User	User IP Ad...	Class	Level	Message
1	2006.01.2...			com.rarita...	WARN	intercept:E...
2	2006.01.2...	ccRoot	192.168.5...	com.rarita...	WARN	execute:e...
3	2006.01.2...	ccRoot	192.168.5...	com.rarita...	WARN	An invalid l...
4	2006.01.2...	ccRoot	192.168.5...	com.rarita...	WARN	An invalid l...
5	2006.01.2...			com.rarita...	WARN	intercept:E...
6	2006.01.2...	ccRoot	192.168.5...	com.rarita...	WARN	execute:e...
7	2006.01.2...			com.rarita...	WARN	intercept:E...
8	2006.01.2...	ccRoot	192.168.5...	com.rarita...	WARN	execute:e...
9	2006.01.2...			com.rarita...	WARN	intercept:E...
10	2006.01.2...	ccRoot	192.168.5...	com.rarita...	WARN	execute:e...
11	2006.01.2...			com.rarita...	WARN	intercept:E...
12	2006.01.2...	ccRoot	192.168.5...	com.rarita...	WARN	execute:e...
13	2006.01.2...	ccRoot	192.168.5...	com.rarita...	WARN	execute:e...
14	2006.01.2...			com.rarita...	WARN	intercept:E...
15	2006.01.2...			com.rarita...	WARN	intercept:E...
16	2006.01.2...	ccRoot	192.168.5...	com.rarita...	WARN	execute:e...
17	2006.01.2...			com.rarita...	WARN	intercept:E...
18	2006.01.2...	ccRoot	192.168.5...	com.rarita...	WARN	execute:e...
19	2006.01.2...			com.rarita...	WARN	intercept:E...
20	2006.01.2...	ccRoot	192.168.5...	com.rarita...	WARN	execute:e...
21	2006.01.2...			com.rarita...	WARN	intercept:E...

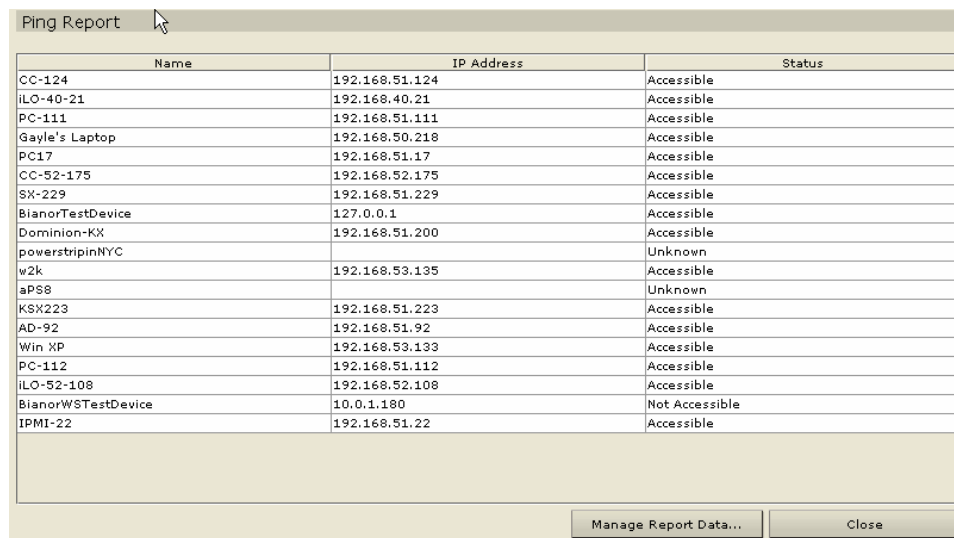
Figure 169 Error Log Report

- Click **Manage Report Data...** to save or print the report. Click **Save** to save the records that are displayed to a CSV file or click **Save All** to save all records. Click **Print** to print the records that are displayed or **Print All** to print all records. Click **Close** to close the window.
- Click **Clear** to clear the contents of the report.
- If the report is lengthy, click **Next** or **Previous** to navigate through the pages.
- Click **Close** to close the **Error Log** report.

Ping Report

The Ping Report displays the status of all connections, showing devices by name and IP address. This report gives you the full accessibility picture for all devices on your system, and will supply information that could be useful in case troubleshooting is necessary.

1. On the **Reports** menu, click **Ping Report**. The **Ping Report** is generated.



The screenshot shows a window titled "Ping Report" with a table containing the following data:

Name	IP Address	Status
CC-124	192.168.51.124	Accessible
iLO-40-21	192.168.40.21	Accessible
PC-111	192.168.51.111	Accessible
Gayle's Laptop	192.168.50.218	Accessible
PC17	192.168.51.17	Accessible
CC-52-175	192.168.52.175	Accessible
SX-229	192.168.51.229	Accessible
BianorTestDevice	127.0.0.1	Accessible
Dominion-KK	192.168.51.200	Accessible
powerstripinNYC		Unknown
w2k	192.168.53.135	Accessible
aPS8		Unknown
KSX223	192.168.51.223	Accessible
AD-92	192.168.51.92	Accessible
Win XP	192.168.53.133	Accessible
PC-112	192.168.51.112	Accessible
iLO-52-108	192.168.52.108	Accessible
BianorWSTestDevice	10.0.1.180	Not Accessible
IPMI-22	192.168.51.22	Accessible

At the bottom of the window, there are two buttons: "Manage Report Data..." and "Close".

Figure 170 Ping Report

2. Click **Manage Report Data...** to save or print the report. Click **Save** to save the report to a location of your choice or **Print** to print the report. Click **Close** to close the window.
3. Click **Close** to close the **Ping Report**.

Accessed Devices Report

Run the Accessed Devices report to view information about any accessed devices, when they were accessed, and the user who accessed them. Filters will help you define the search criteria for a more concise report.

1. On the **Reports** menu, click **Accessed Devices**. The **Accessed Devices** screen appears.

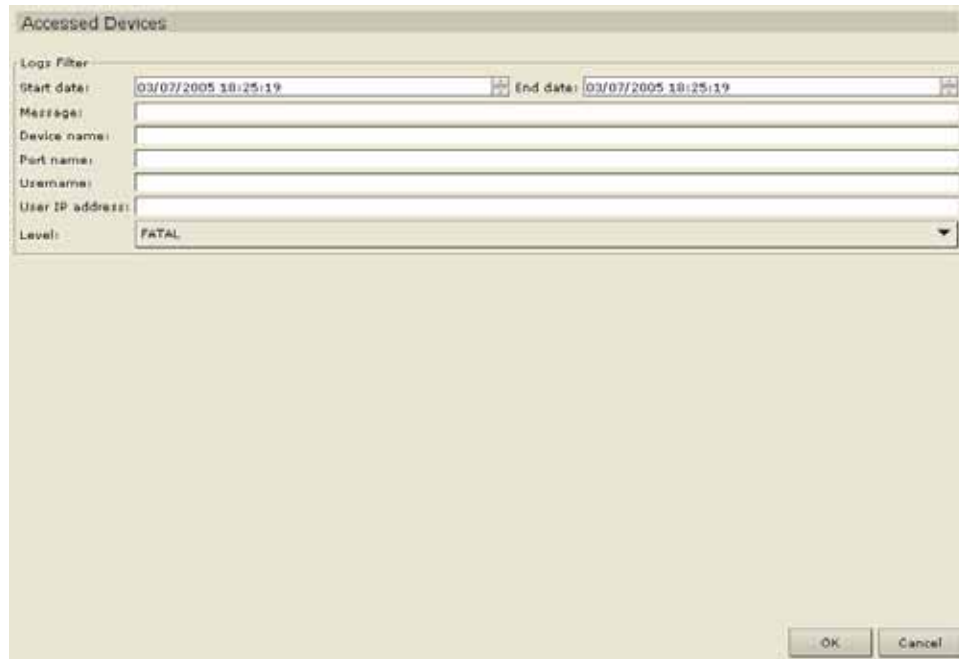
The screenshot shows a web-based interface titled "Accessed Devices". It features a "Logs Filter" section with several input fields: "Start date:" and "End date:" both containing "03/07/2005 10:25:19"; "Message:"; "Device name:"; "Port name:"; "Username:"; and "User IP address:". Below these is a "Level:" dropdown menu currently set to "FATAL". At the bottom right of the form are "OK" and "Cancel" buttons.

Figure 171 Accessed Devices Screen

2. Select the date range for the report by either typing the date and time in the **Start Date** and **End Date** fields using the format **yyyy/mm/dd hh:mm:ss**, or by using the <→> key on your keyboard to advance through the sections and click on the up/down arrows to build the date and time.
3. Type the criteria with which to filter the report in the **Message**, **Device Name**, **Port Name**, **Username**, or **User IP address** fields.
4. Click on the **Level** drop-down arrow to select a tracing level for the report.

- Click **OK** to run the report.

Accessed Devices							
No.	Date	Device	Port	User	User IP A...	Message	Level
1	2006-01-...	kx-132-e...	Channel 3	ccRoot	192.168...	Connecti...	INFO
2	2006-01-...	kx-132-e...	Channel 3	ccRoot	192.168...	Connecti...	INFO
3	2006-01-...	kx-132-e...	Channel 3	ccRoot	192.168...	Connecti...	INFO
4	2006-01-...	kx-132-e...	Channel 1	ccRoot	192.168...	Connecti...	INFO
5	2006-01-...	kx-132-e...	Channel 1	ccRoot	192.168...	Connecti...	INFO
6	2006-01-...	kx-132-e...	Channel 1	ccRoot	192.168...	Connecti...	INFO
7	2006-01-...	kx-132-e...		ccRoot	192.168...	Connecti...	INFO
8	2006-01-...	kx-132-e...		ccRoot	192.168...	Connecti...	INFO
9	2006-01-...	kx-132-e...		ccRoot	192.168...	Connecti...	INFO
10	2006-01-...	kx-132-e...		ccRoot	192.168...	Connecti...	INFO
11	2006-01-...	kx-132-e...		ccRoot	192.168...	Connecti...	INFO
12	2006-01-...	kx-132-e...		ccRoot	192.168...	Connecti...	INFO
13	2006-01-...	kx-132-e...		ccRoot	192.168...	Connecti...	INFO
14	2006-01-...	kx-132-e...		ccRoot	192.168...	Connecti...	INFO
15	2006-01-...	kx-132-e...		ccRoot	192.168...	Connecti...	INFO
16	2006-01-...	kx-132-e...		ccRoot	192.168...	Connecti...	INFO
17	2006-01-...	kx-132-e...		ccRoot	192.168...	Connecti...	INFO
18	2006-01-...	kx-132-e...		ccRoot	192.168...	Connecti...	INFO
19	2006-01-...	kx-132-e...		ccRoot	192.168...	Connecti...	INFO
20	2006-01-...	kx-132-e...		ccRoot	192.168...	Connecti...	INFO

Previous

Next

Manage Report Data... Clear Close

Figure 172 Accessed Devices Report

- The Accessed Devices report is generated, displaying data about devices accessed during the designated time period.
- Click **Manage Report Data...** to save or print the report. Click **Save** to save the records that are displayed to a CSV file or click **Save All** to save all records. Click **Print** to print the records that are displayed or **Print All** to print all records. Click **Close** to close the window.
- Click **Clear** to clear the contents of the report.
- If the report is lengthy, click **Next** or **Previous** to navigate through the pages.
- Click **Close** to close the **Accessed Devices** report.

Group Data Report

The Group Data report displays user, port, and device Group information. View user groups by name and description, view port groups by name, and view device groups by name, all in one screen.

1. On the **Reports** menu, click **Group Data**. The **Groups** report is generated. Use the scroll bars to scroll through the lists and view all entries.

The screenshot shows a window titled "Groups" with three main sections, each containing a table and a "Manage Report Data..." button.

User Groups Section:

User Group Name	Group Description	Privileges	Policies
AllPowerXUsers	Testing user management	CC Setup And Control, D...	...
ccadgroup1	Imported from LDAP.	Ports Access	Full Access Policy
CC User		Ports Access	...
CharlieGroup		Device And Port Manage...	...

Port Groups Section:

Port Group Name	Full Rule String
All Ports	Port Name LIKE %
cleaner Ports	New Look UI Cat = cleaner
Clearer Ports	Another UI Cat = Clearer
clear Ports	UI Cat = clear

Device Groups Section:

Device Group Name	Full Rule String
All Devices	Device Name LIKE %
KSX-devices	Device Type = Dominion KSX
kx-224-1	Device Name = KX-224-1

At the bottom of the window are two buttons: "Manage Report Data..." and "Close".

Figure 173 Groups Report

2. Click on the ... button next to a line entry to display either the policies associated with the user group, or the list of ports that satisfy the port group rule, or the list of devices that satisfy the device group rule.
3. Click any of the **Manage Report Data...** buttons to save or print the report for any particular section. Click **Save** to save the report to a location of your choice or **Print** to print the report. Click **Close** to close the window.
4. Click **Close** to close the **Groups** report.

User Data Report

The User Data report displays certain data on all users in the CC-SG database. From **User Name** field you can see names of users currently in session and view details of users currently not in session. From **Phone** field you can see user dial back telephone number. From **Enabled** field you can see information if check box **Login** is enabled. From **Password Expiration** you can see password expiration period in days.

1. On the **Reports** menu, click **User Data**. The **All Users' Data** report is generated. Use the scroll bar to scroll through the list and view all entries.

User Name	Phone	Enabled	Password Expir...	Groups	Privileges	Email	User Type
chucktest	102	true		CC Users	Ports Access		local
PatPublic	102	true		Charlie'sAngels	Ports Access		local
kensearcy	102	true		CC Users	Ports Access		local
kenny	102	true		System Admin...	CC Setup And ...		local
cdef	102	true					remote
kunal	102	true					local
BianorTestUser	102	true		System Admin...	CC Setup And ...		local
Qing	102	true		System Admin...	CC Setup And ...	qing@raritan.c...	local
mistermister	102	true		CC Users	Ports Access		local
charliem	102	true		KG User Group	CC Setup And ...		remote
tester	102	true		System Admin...	CC Setup And ...		local
MrExpiration	102	true	3	Product Manag...	CC Setup And ...		local
MrExpiration1	102	true	19	Product Manag...	CC Setup And ...		local
t123	102	true	1	CC Users	Ports Access		local
test2	102	true					local
charlie	102	true		Product Manag...	CC Setup And ...	charlesme@rar...	local
marshall	102	true		Pre-Windows 2...	Ports Access, ...		local
test	102	true		Pre-Windows 2...	Ports Access		local
admin	102	true		System Admin...	CC Setup And ...		local
Lese	102	true	2	System Admin...	CC Setup And ...	Elizabeth.Lelli...	local
pavel	102	true		System Admin...	CC Setup And ...		local
ccRoot	102	true		System Admin...	CC Setup And ...	cc30admin@ra...	local
navle	102	true		CCSetupandC...	CC Setup And ...		local

Manage Report Data... Close

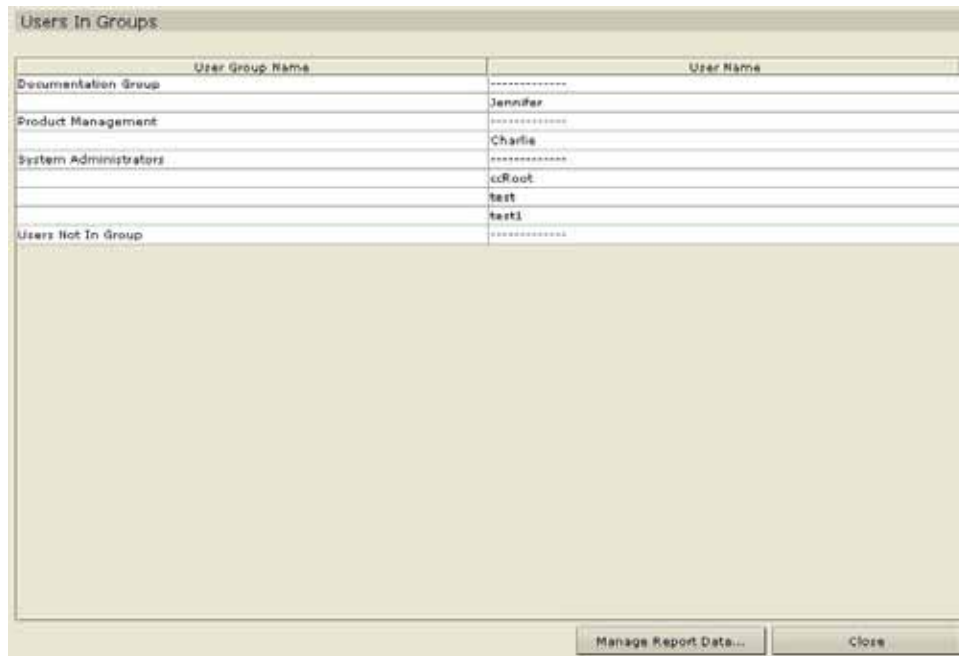
Figure 174 All Users' Data Report

2. Click **Manage Report Data...** to save or print the report. Click **Save** to save the report to a location of your choice or **Print** to print the report. Click **Close** to close the window.
3. Click **Close** to close the **All Users' Data** report.

Users In Groups Report

The Users In Group report displays data on users and the groups with which they are associated.

1. On the **Reports** menu, click **Users In Groups**. The **Users In Groups** report is generated. Use the scroll bar to scroll through the list and view all entries.



User Group Name	User Name
Documentation Group	Jennifer
Product Management	Charlie
System Administrators	ccRoot
	test
	test1
Users Not In Group	

Figure 175 Users In Groups Report

2. Click **Manage Report Data...** to save or print the report. Click **Save** to save the report to a location of your choice or **Print** to print the report. Click **Close** to close the window.
3. Click **Close** to close the **Users In Groups** report.

Query Port Report

The Query Port Report displays all ports according to port status.

1. On the **Reports** menu, click **Query Port**. The **Query Port** screen appears.

Figure 176 Query Port Report

2. Click on one or more checkboxes to customize the port information you want to see in the report.

PORT STATUS	DEFINITION
New	Port is available (physical connection to target server is in place), but the port has not been configured. Click Configure next to the port in the report to configure it now.
Unused	Port is unavailable (physical connection to target server is not in place) and the port has not been configured. Click Configure next to the port in the report to configure it now if the device is available.
Available	Port has been configured and connection to port is possible.
Unavailable	Connection to port is not possible since the device is down and unavailable.
Busy	A user is connected to this port.

3. Click **Apply** to generate the report. Checking more than one checkbox and clicking **Apply** will display ports with ALL statuses that are selected.
4. Check the **Show Ghosted Ports** checkbox in conjunction with one or more port statuses to display ports that have the selected port status in addition to being *ghosted*. A ghosted port can occur when managing Paragon devices and when a CIM or target server is removed from the system or powered off (manually or accidentally). Refer to Raritan's *Paragon II User Manual* for additional information.
5. Click on any of the column headers to sort the ports by that attribute in ascending order. Click on the header again to sort the ports in descending order.
6. Click **Close** to close the **Query Port** report.

View Stored Reports

The View Stored Reports displays reports that were scheduled in the Task Manager—see section **Task Manager** in **Chapter 12: Advanced Administration**.

1. On the **Reports** menu, click **View Stored Reports**.

The screenshot shows the 'Scheduled Reports' window. At the top, there is a 'Report Filter' section with the following fields:

- Report Type:** All (dropdown menu)
- Report Owner:** All (dropdown menu)
- Reports generated between:** 10/31/2004 14:07:56 and 11/01/2005 15:05:20 (date and time pickers)
- Report Name (by phrase):** (text input field)

A 'Get Reports' button is located to the right of the filter fields. Below the filter section is a table with the following data:

Report Type	Generation Date	Owner	Task Name
Active Users Report	2005.10.28 at 15:15:11 EDT	ccRoot	Active Users1
Error Log Report	2005.10.27 at 12:50:47 EDT	ccRoot	Error Logs
Active Users Report	2005.10.28 at 15:15:11 EDT	ccRoot	Active Users
Active Users Report	2005.10.29 at 15:15:11 EDT	ccRoot	Active Users
Active Users Report	2005.10.30 at 15:15:11 EST	ccRoot	Active Users
Active Users Report	2005.11.01 at 12:10:00 EST	ccRoot	
Active Users Report	2005.10.24 at 14:31:12 EDT	ccRoot	
Audit Trail Report	2005.10.24 at 14:32:04 EDT	ccRoot	
Group Data Report	2005.10.28 at 15:31:00 EDT	ccRoot	Test
Active Ports Report	2005.10.27 at 15:31:33 EDT	ccRoot	
Active Users Report	2005.10.29 at 15:15:11 EDT	ccRoot	Active Users

At the bottom right of the window are 'Show Report' and 'Close' buttons.

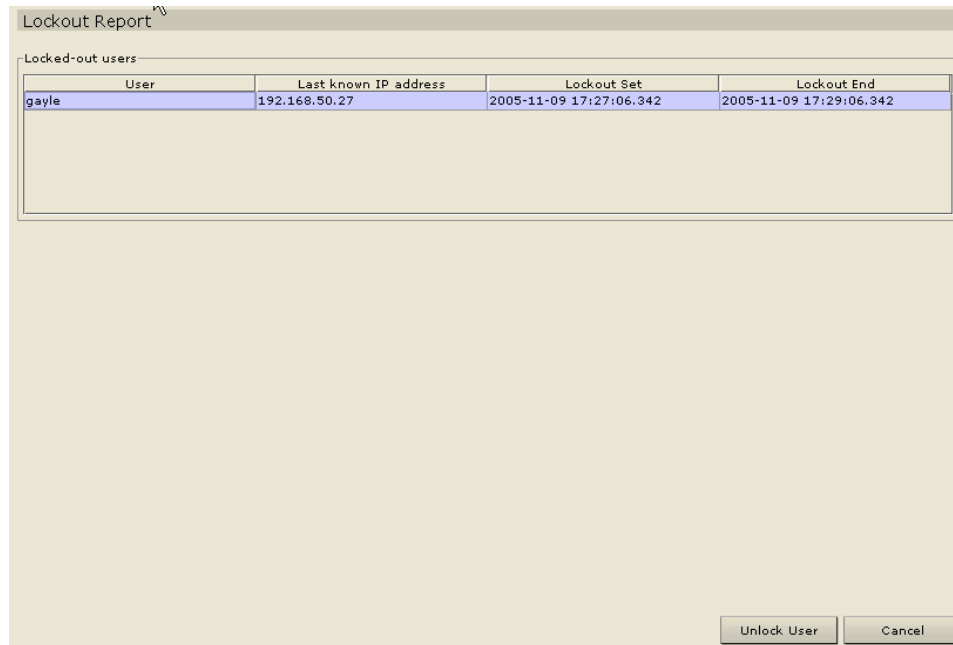
Figure 177 View Stored Reports

2. Click **Get Reports** to view the entire list of all scheduled reports that were created by all owners. By default, all reports that were scheduled an hour ago to the current time are displayed.
3. To filter the reports displayed, you can select a particular **Report Type**, such as Active Ports Report, or **Report Owner** or alter the start and end dates in **Reports generated between** by highlighting the month, date, year, or time fields and clicking the or buttons. Also, you can enter a **Report Name** to filter on the name—enter a phrase or partial phrase of the name; matches are case in-sensitive and wildcards are not allowed. Click **Get Reports** to view the filtered list.
4. Click on any of the column headers to sort the ports by that attribute, such as **Report Type**, in ascending order. Click on the header again to sort the ports in descending order.
5. To view an individual report, highlight the report in the list and click **Show Report**.

Locked Out Users Report

The Locked Out Users report displays users who are currently locked out of CC-SG. You can unlock them from this report.

1. On the **Reports** menu, click **Locked Out Users**.



User	Last known IP address	Lockout Set	Lockout End
gayle	192.168.50.27	2005-11-09 17:27:06.342	2005-11-09 17:29:06.342

Unlock User Cancel

Figure 178 Locked Out Users Report

2. Highlight the user you want to unlock and click **Unlock User**. An email notification is sent to the email address that was specified during lockout configuration. For more information on how to enable lockout, please see section **Enable User Lockout** in **Chapter 12: Advanced Administration**.

CC-NOC Synchronization Report

The CC-NOC Synchronization report lists all targets, along with their IP addresses, that the CC-SG subscribes to and are monitored by a CC-NOC given a particular discovery date. Any new targets that are discovered in the configured range are displayed here as well. See **Add a CC-NOC** in **Chapter 12: Advanced Administration** for details. You can also purge targets from the CC-SG database from this report.

1. On the **Reports** menu, click **CC-NOC Synchronization**.

Name	Host/IP Address	Last Discovered Date	CC-NOC IP Address
------	-----------------	----------------------	-------------------

Figure 179 CC-NOC Synchronization Report

2. Select a **Last Discovered Date** and click **Get Targets**. The targets that were discovered on or earlier than the **Last Discovered Date** are displayed under **Targets Discovered**.
3. You can purge some of the targets from the CC-SG database by highlighting them and clicking **Purge** or purge the entire list by clicking **Purge All**. If a generic device is associated with the target, it too will be purged.
4. Click **Manage Report Data...** to print the list of targets or save them in a CSV formatted file.

Chapter 11: System Maintenance

Reset CC-SG

Use the Reset CommandCenter command to reset CC-SG database data – please note that this command will not reset system configuration data, such as the IP address of CC-SG.

1. On the **Setup** menu, click **Reset CommandCenter**.

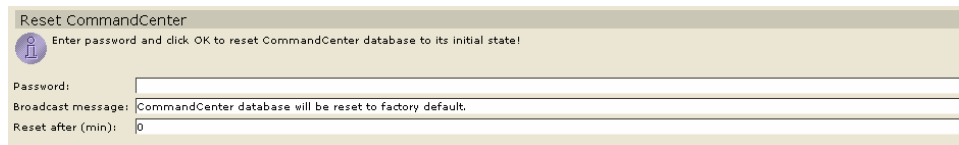


Figure 180 Reset CC-SG Screen

2. Type your CC-SG **password**.
3. Either accept the current **Broadcast message** or edit to create one of your own.
4. Type the number of minutes in which to wait until CC-SG is reset in **Reset after (min)**. Default is 0, which will reset the CC-SG unit immediately.
5. Click **OK** to reset your CC-SG unit. A success message will appear to confirm the reset.

Important: Using the Reset command will flush the database of CC-SG. All Devices, Ports, and Users will be removed from the CC-SG. Authentication is also reset to using Local DB. You should back up the CC-SG before using Reset.

Backup CC-SG

1. On the **Setup** menu, click **Backup CommandCenter**.
2. When the **Backup CommandCenter** screen appears, if desired, check **Do not backup logs** if you do not want the log files backed up. Also check **Do not backup firmware binaries** if you do not want the device firmware binaries to be backed up. Checking these options saves time and disk space.

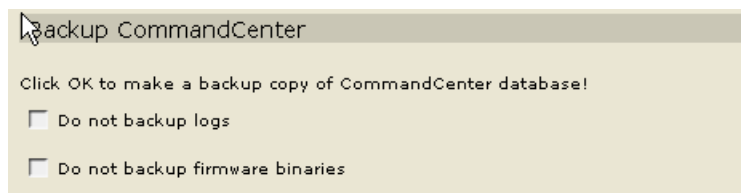


Figure 181 Backup CC-SG Screen

3. Click **OK**. The backup file will be saved in the CC-SG file system, and can be restored at a later time and a success message will appear to confirm CC-SG backup.

Restore CC-SG

1. On the **Setup** menu, click **Restore CommandCenter**.
2. When the **Restore CommandCenter** screen appears, choose if you want to click on the backup that you want to restore to your CC-SG unit, and then click **OK**.

The screenshot shows the 'Restore CommandCenter' window. It contains a table with the following data:

Date	Name	Data Version	Info	Size
Wed Dec 21 14:47:04 EST...	backup_21_12_2005_14_...	3.0.0.2.4	CommandCenter backup ...	30037kB
Mon Dec 19 15:55:24 EST...	backup_19_12_2005_15_...	3.0.0.2.4	CommandCenter backup ...	17541kB
Thu Dec 15 12:44:00 EST...	backup_15_12_2005_12_...	3.0.0.2.3	CommandCenter backup ...	17600kB
Thu Dec 15 12:54:44 EST...	backup_15_12_2005_12_...	3.0.0.2.4	CommandCenter backup ...	17585kB
Mon Dec 05 12:14:34 EST...	backup_05_12_2005_12_...	3.0.0.2.2	CommandCenter backup ...	13230kB
Fri Dec 30 21:36:28 EST ...	backup_30_12_2005_21_...	3.0.0.2.4	CommandCenter backup ...	17557kB
Tue Dec 13 16:26:41 EST...	backup_13_12_2005_16_...	3.0.0.2.3	CommandCenter backup ...	17593kB
Wed Dec 21 14:22:22 ES...	backup_21_12_2005_14_...	3.0.0.2.4	CommandCenter backup ...	17569kB
Fri Dec 30 10:20:20 EST ...	backup_30_12_2005_10_...	3.0.0.2.4	CommandCenter backup ...	17534kB

Below the table are three checkboxes:

- ☐ Do not restore logs
- ☐ Restore Data only
- ☐ Restore Firmware binaries

At the bottom, there is a 'Broadcast message' field containing 'CommandCenter will be restored.' and a 'Restore after (min):' field with the value '0'. On the right side, there are five buttons: 'Upload', 'Download', 'Remove', 'OK', and 'Close'.

Figure 182 Restore CC-SG Screen

3. When the **Restore CommandCenter** screen appears, check **Do not restore logs** if you do not want the log files restored. Check **Restore Data only** if you only want the configuration data (devices, ports, users) restored. Check **Restore Firmware binaries** if you want the device firmware files restored.
4. Click on the backup that you want to restore to your CC-SG unit, and then click **OK**.
5. If you want to download a backup and restore it in another CC-SG unit, select a backup and click **Download**. Then on the CC-SG unit you want to apply the backup, click **Upload** to restore the backup on that unit.

Saving and Uploading Backup Files

You can also save and load CC-SG backups to and from your local PC using the **Restore CommandCenter** screen.

1. Click on the backup you wish to save to your PC, and then click **Download**.
2. Specify a location to save your CC-SG backup file.
3. To upload a backup to a CC-SG unit, click **Upload** on the **Restore CommandCenter** screen and browse your system for the backup of your CC-SG configuration.

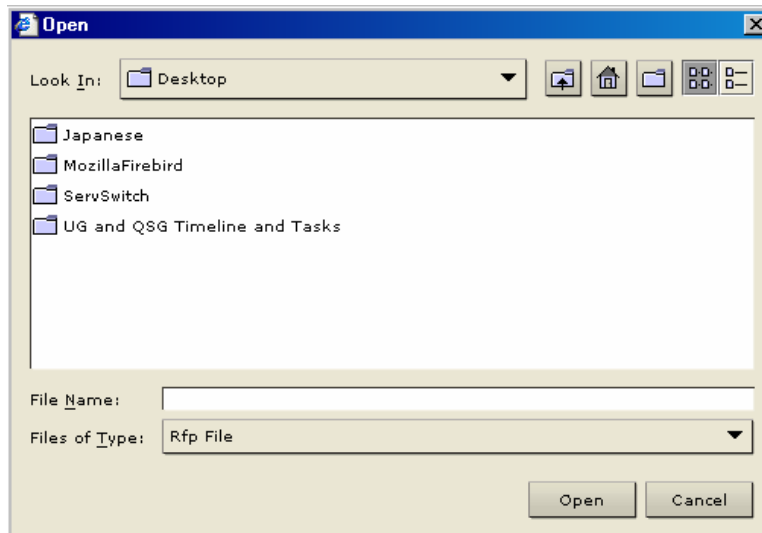


Figure 183 Browse to Upload a Backup of CC-SG

4. When you have located the file, click **Open** to add it to the list of available backups on your CC-SG server.

Note: Saving and restoring can be used to move a backup from one CC-SG unit to another.

Refresh CC-SG Display

Any edits or modifications made to users, ports, categories, elements, and other system components are not reflected in the system until the database is updated. If you are logged in while another user is updating the database, you will not see these changes unless you refresh your screen (or log out of CC-SG and log back in).

1. Click on the **Refresh** shortcut button in the CC-SG toolbar to refresh your browser.

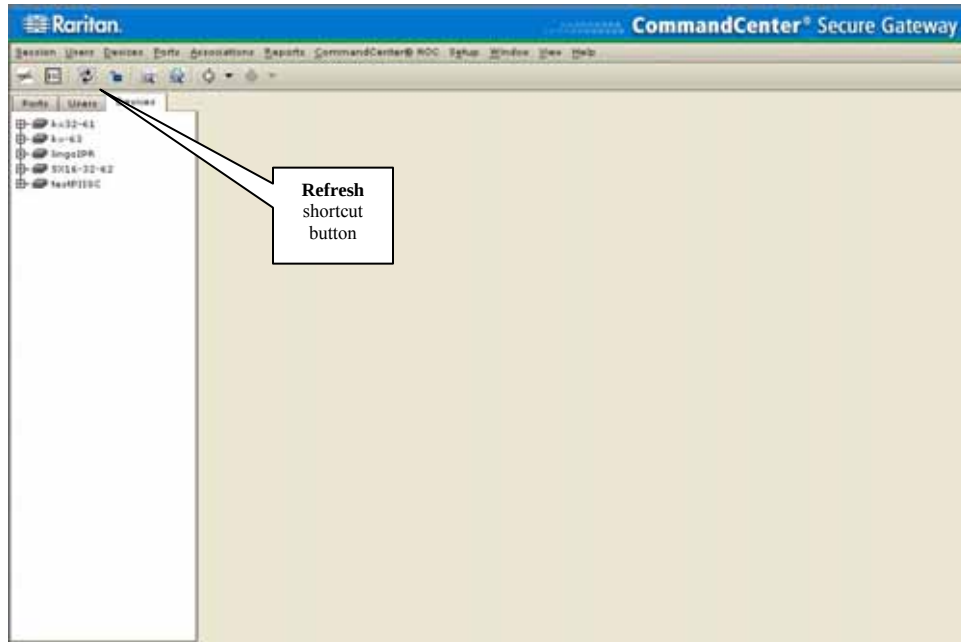


Figure 184 Refresh Shortcut Button

Upgrade CC-SG

Note: If you are operating a CC-SG cluster, you must remove the cluster first and upgrade each node separately. Before you can upgrade CC-SG, you must be in Maintenance Mode. See section **Maintenance Mode** in **Chapter 11: System Maintenance** for additional information.

1. On the **Setup** menu, click **Upgrade CommandCenter**. The **Upgrade CommandCenter** screen appears.



Figure 185 Upgrade CC-SG Screen

2. If you are upgrading from an older CC-SG, click **Browse** and navigate to the current location of your CC files.
3. Click **OK**.

Restart CC-SG

1. On the **Setup** menu, click **Restart CommandCenter**. The **Restart CommandCenter** screen appears.

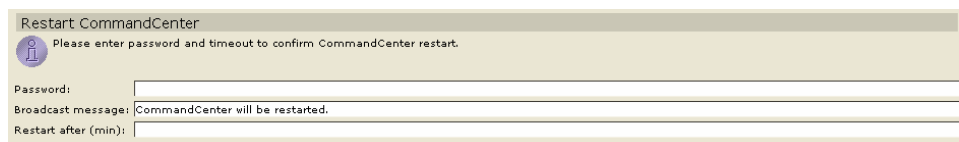


Figure 186 Restart Screen

2. Type your password in the **Password** field.
3. Accept the default message or type a message to display to any users currently online in the **Broadcast message** field (for example, you might give users a brief time period to finish their tasks in CC-SG or tell them why you are restarting the system). All users will be disconnected when you restart CC-SG.
4. Type how much time (in minutes) should pass before CC-SG restarts in the **Restart after (min)** field.

- Click **OK** to restart CC-SG or **Cancel** to exit the screen without restarting. Once you restart CC-SG, your Broadcast Message appears.

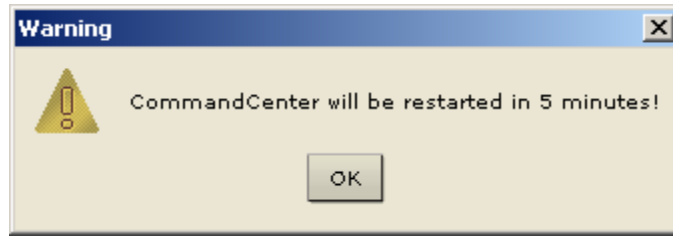


Figure 187 Info Window

- Click **OK** to restart CC-SG.
- CC-SG will restart, and is ready for use.

Shut Down CC-SG

These are the recommended methods for Administrators to shut down and restart CC-SG.

- On the **Setup** menu, click **Shutdown CommandCenter**. The Shutdown CommandCenter screen appears.

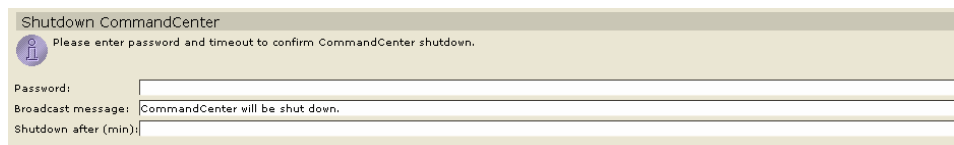


Figure 188 Shutdown CC-SG Screen

- Type your password in the **Password** field.
- Accept the default message or type a message to display to any users currently online in the **Broadcast message** field (for example, you might give users a brief time period to finish their tasks in CC-SG and tell them when they can expect the system to be functional again). All users will be disconnected when you shutdown CC-SG.
- Type how much time (in minutes) should pass before CC-SG shuts down in the **Shutdown after (min)** field.
- Click **OK** to shut down CC-SG or **Cancel** to exit the screen without shutting down. Once you shut down, the CC-SG login window appears.

Log on to CC-SG again to continue working, or click **Exit** on the login screen to close the browser. You can also shut CC-SG down from SSH – please see section **SSH Access to CC-SG** in **Chapter 12: Advanced Administration** for additional information.

Restart CC-SG after Shutdown

After shutting down CC-SG, use one of these two methods to restart the unit:

- Use the Diagnostic Console – please see section **Diagnostic Console** in **Chapter 12: Advanced Administration** for additional information.
- Recycle the power to your CC-SG unit.

End CC-SG Session

Log Out

To exit CC-SG at the end of a session, or to refresh the database in case you or another user has made changes while you were logged in, log off from CC-SG entirely, then log in again.

1. On the **Session** menu, click **Logout**. The **Logout** window appears.

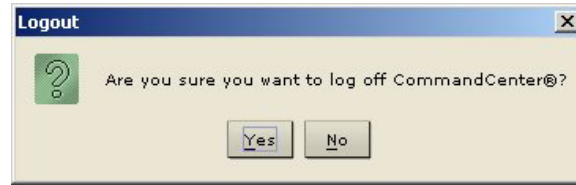


Figure 189 Logout Window

2. Click **Yes** to log out of CC-SG or **No** to close the window. Once you log out, the CC-SG login window appears.
3. Log on to CC-SG again, or click **Exit** to shut down CC-SG completely.

Exit CC-SG

If at any time you want to exit CC-SG, you can exit.

1. On the **Session** menu, click **Exit**. The **Exit** window appears.

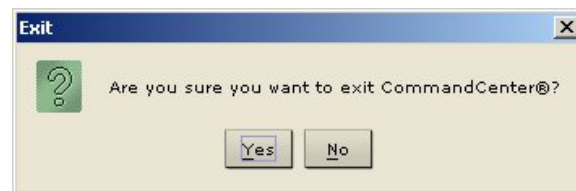


Figure 190 Exit Window

2. Click **Yes** to exit CC-SG or **No** to close the **Exit** window and continue working.

Maintenance Mode

This mode restricts access to CC-SG so that an administrator can perform various operations without disruption. Operations can be performed from the GUI or from an SSH command line interface via clients, such as Putty, OpenSSH Client, etc. Please see **Chapter 12: Advanced Administration, SSH Access** for additional information.

Current users, except the administrator who is initiating Maintenance Mode, are alerted and logged out after the configurable time period expires. While in Maintenance Mode, other administrators are allowed to log into CC-SG, but non-administrators are prevented from logging in. An SNMP trap is generated each time CC-SG enters or exits Maintenance Mode.

Note: Maintenance Mode is only available on standalone CC-SG's and not in a cluster configuration.

Scheduled Tasks

Scheduled tasks cannot execute while CC-SG is in Maintenance Mode—please see section **Task Manager** in **Chapter 12: Advanced Administration** for additional information on scheduled tasks. When CC-SG exits Maintenance Mode, scheduled tasks will be executed as soon as possible.

Entering Maintenance Mode

To enter Maintenance Mode:

1. On the **Setup** menu, click **Maintenance Mode**.
2. Click **Enter Maintenance Mode**.

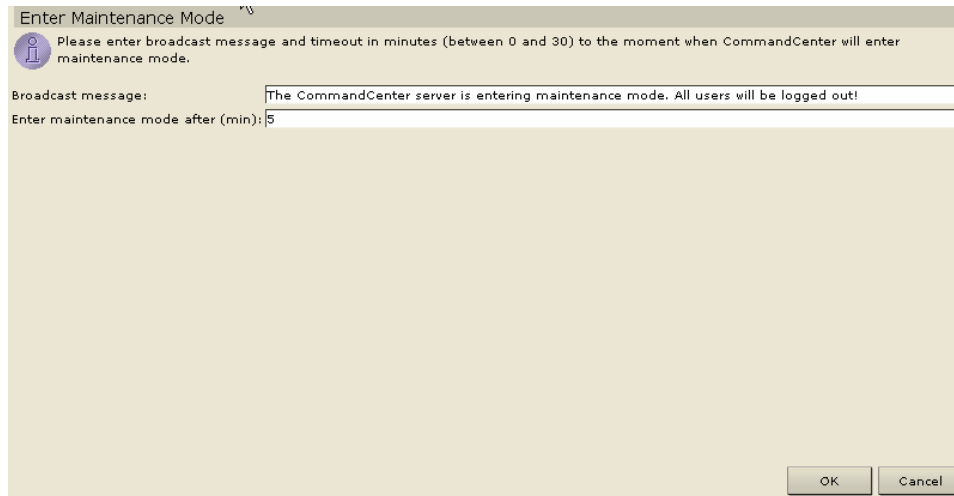


Figure 191 Enter Maintenance Mode

3. Type a **broadcast message** or accept the default that is provided.
4. Type a number that will start a count down clock on each CC-SG client. Type a number between **0** and **30**. Default is **5**. Typing **0** means that Maintenance Mode is starting immediately.
5. Click **OK**.

Exiting Maintenance Mode

To exit Maintenance Mode:

1. On the **Setup** menu, click **Maintenance Mode**.
2. Click **Exit Maintenance Mode**.

Chapter 12: Advanced Administration

Configuration Manager

Network Configuration

1. On the **Setup** menu, click **Configuration Manager**. When the **Configuration Manager** screen appears, click on the **Network Setup** tab.

Figure 192 Configuration Manager Network Settings Screen

2. Type the CC-SG hostname in the **Host Name** field. For hostname rules, see **Terminology/Acronyms** in **Chapter 1: Introduction**. Once **Update Configuration** is selected, the field will be updated to reflect the Fully-Qualified Domain Name (FQDN) if a domain server and domain suffix has been configured.
3. Click either **Primary/Backup Mode** or **Active/Active Mode**. A standard CC-SG provides two Network Interface Controllers (NIC)s. The NICs (labeled left-to-right from the rear) are as follows:

MODEL	LEFT-MOST NIC (PRIMARY INTERFACE)	RIGHT-MOST NIC
G1	LAN1	LAN0
V1	LAN1	LAN2

One interface could be used by itself or both could be used simultaneously. For simplicity, the discussion below uses LAN1 as the left-most NIC (primary) and LAN2 as the right-most NIC. Some internal diagnostics and messages may refer to these interfaces as “eth0” and “eth1”.

Note: If both interfaces are disconnected, CC-SG restarts.

- A. Choose **Primary/Backup mode** to implement network failover and redundancy. In this mode, only one NIC is active at a given point of time and only one network IP address assignment is possible.

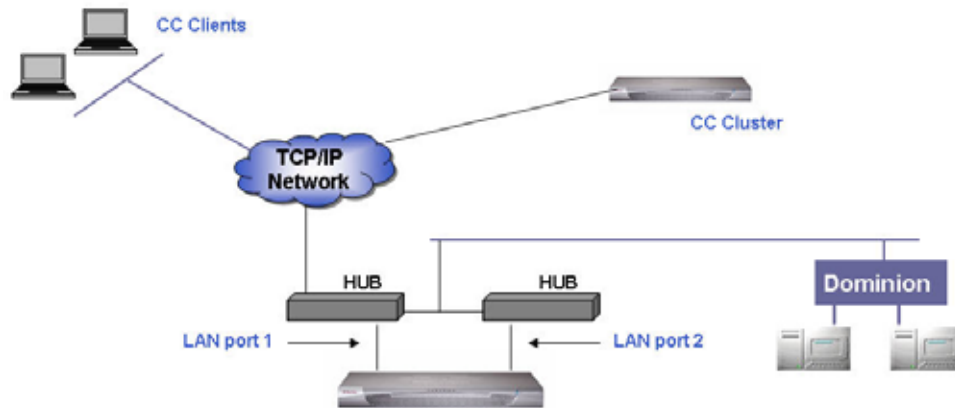


Figure 193 Primary/Backup Network

Typically, both NICs are attached to the same LAN sub-network, but different switches (or hubs) may be used for reliability. When both NICs are used, a level of network redundancy is provided. For example, if LAN1 is connected and is receiving a Link Integrity signal, CC-SG uses this NIC for all communications. In the event of a LAN1 failure and assuming LAN2 is connected, CC-SG migrates the assigned (possibly by DHCP) IP address to LAN2. LAN2 will be used until LAN1 is repaired and returned to service. When this happens, CC-SG reverts to using LAN1.

As long as one interface is viable, a PC client should not notice any disruption in service during a failure. CC-SG remains at the same logical IP address, but attempts to keep communication channels and existing sessions up in the event of possible network failures. All communication (for example, PC client, Raritan device management, cluster peer, etc.) is carried over this single communication channel that is maintained by both NICs.

- B. Choose **Active/Active mode** if you have special network conditions; particularly if you have two networks where routing may not exist. If network security is important and if you are using proxy-type deployments, you also should choose this mode.

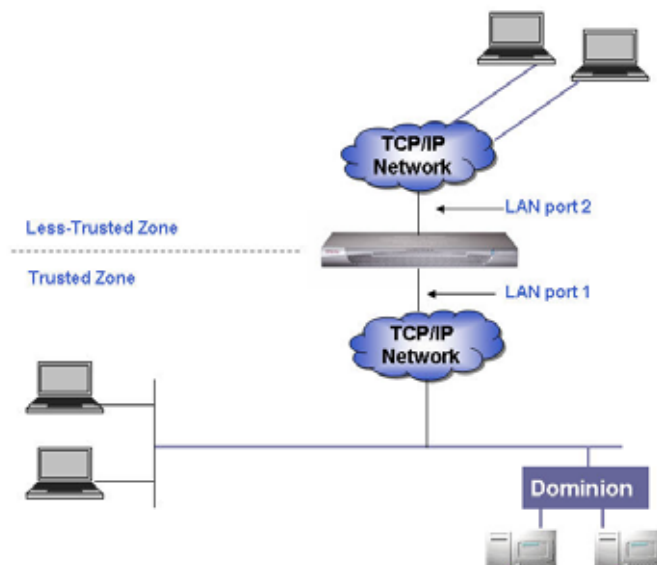


Figure 194 Active/Active Network

In this mode, CC-SG acts as a “router” or “traffic cop” between two separate IP domains; particularly when **Proxy** mode is being used (please see **Connection Mode**, later in this chapter, for additional information). In Proxy mode, **Active/Active** mode is required so CC-SG routes proxied PC client sessions to their respective end-points. It is recommended that Raritan-controlled devices be connected to LAN1 while proxied PC client connections are connected to LAN2. Both NICs should be on separate sub-networks—however, if you are using DHCP, this may not be possible and therefore it would not be a supported configuration. While configuring both NICs, specify a default gateway address for only one NIC and leave the other blank.

When a NIC fails, CC-SG attempts to route the packet from the other NIC based on the current IP routing table. This routing may not be successful, especially if firewalls are involved. If additional routes are needed, they can be added in Diagnostic Console (please see Editing Static Routes (Network Interfaces), later in this chapter, for additional information).

Note: *Clustering cannot be configured when using **Active/Active** mode.*

4. Click on the **Configuration** drop-down arrow and select either **DHCP** or **Static** from the list. If you choose **DHCP** and your DHCP server has been configured correctly, then type a hostname and select DHCP from the Configuration drop-down arrow. The DNS information, the domain suffix, IP address, default gateway and subnet mask, will be automatically populated once Update Configuration is selected. With this information, CC-SG registers itself dynamically with the DNS server if it accepts dynamic updates. After a successful registration, CC-SG can be accessed via the hostname since the IP address may not be known when using DHCP. If you choose **Static**, type an **IP address**, **subnet mask**, **default gateway**, **Primary DNS** and **Secondary DNS** information, and string for your domain setup in **domain suffix**.
5. Click on the **Adapter Speed** drop-down arrow and select a line speed from the list.
6. Click on the **Adapter Mode** drop-down arrow and select a duplex mode from the list, if applicable.
7. Click **Update Configuration** to update the Network Setup of your system.
8. Click **Close** to close the **Configuration Manager** screen.

Log Configuration

1. On the **Setup** menu, click **Configuration Manager**. When the Configuration Manager screen appears, click on the **Logs** tab.

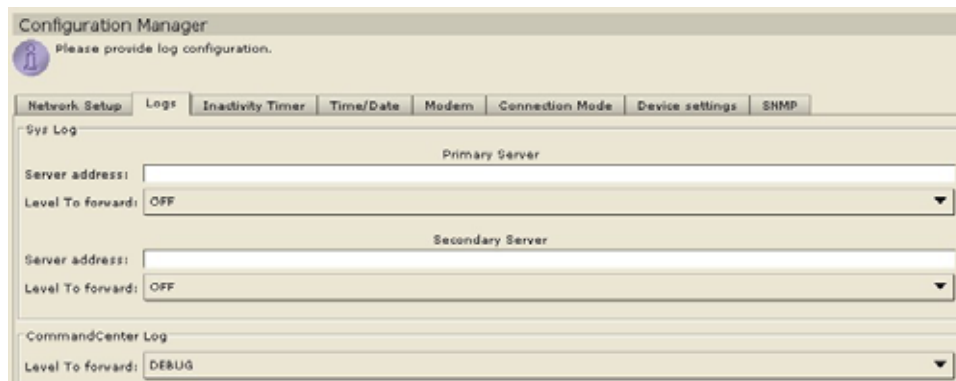


Figure 195 Configuration Manager Logs Screen

2. Type IP addresses into the **Server Address** field.

3. Click on the **Level to Forward** drop-down arrow to select a level.
4. Repeat steps 2 and 3 for Secondary Server fields (note that Secondary Server is optional).
5. Click **Update Configuration** to save the server addresses to the system.
6. Click **Close** to close the Configuration Manager screen.

Inactivity Timer Configuration

Use this screen to time out inactive user sessions.

1. On the **Setup** menu, click **Configuration Manager**. When the **Configuration Manager** screen appears, click on the **Inactivity Timer** tab.

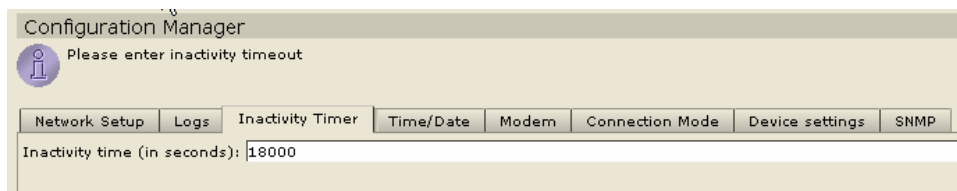


Figure 196 Configuration Manager Inactivity Timer Screen

2. Type the desired time limit for inactivity in the **Inactivity Time (in seconds)** field.
3. Click **Update Configuration** to apply the changes to the system.
4. Click **Close** to close the **Configuration Manager** screen.

Time/Date Configuration

CC-SG's Time and Date stamps must be accurately maintained in order to provide credibility for its device-management capabilities.

Important! This time is used when scheduling tasks in Task Manager—see section Task Manager in Chapter 12: Advanced Administration. The time set on the client may be different than the time set on CC-SG.

Only Administrators and ccroot users can synchronize Time and Date.

1. On the **Setup** menu, click **Configuration Manager**. When the **Configuration Manager** screen appears, click on the **Time/Date** tab.

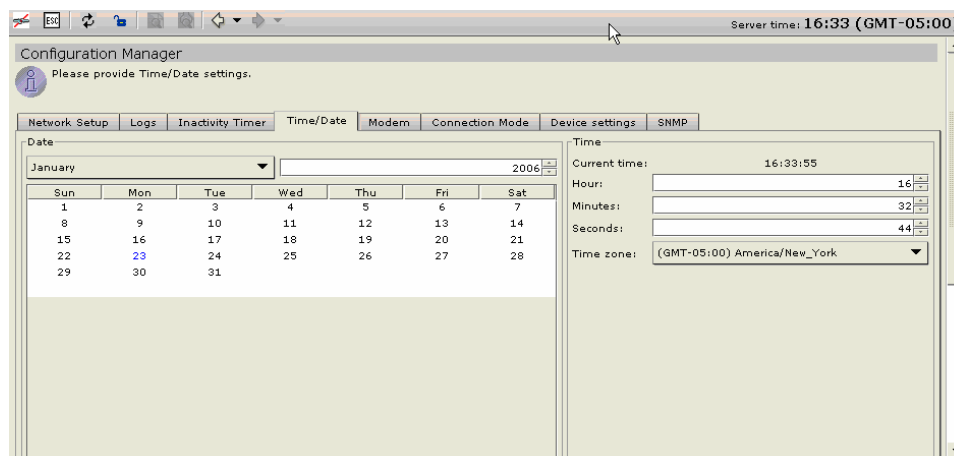


Figure 197 Configuration Manager Time/Date Screen

- a. To set the date and time manually: To set the **Date**, click on the drop-down arrow to select the Month, use the up/down arrows to select the Year, and click on the Day in the calendar area. To set the **Time**, use the up/down arrows to set the **Hour**, **Minutes**, and **Seconds**, and then click on the **Time Zone** drop-down arrow to select the time zone in which you are operating CC-SG.
- b. To set the date and time via NTP: Click on the **Enable Network Time Protocol** check box at the bottom of the window and enter the IP addresses for both the **Primary** (NTP) **Server** and the **Secondary** (NTP) **Server**.

Note: Network Time Protocol (NTP) is the protocol used to synchronize the attached computers' date and time data with a referenced NTP server. When CC-SG is configured with NTP, it can synchronize its clock time with the publicly available NTP reference server and maintain correct and consistent time.

2. Click **Update Configuration** to apply the time and date changes to CC-SG.
3. Click **Refresh**  in the upper-left portion of the window to see the new **Server time** reflected on your client GUI as seen in the screen above.
4. Click **Close** to close the **Configuration Manager** screen.
5. On the **Setup** menu, click **Restart CommandCenter**.

Note: Changing the time zone is disabled in a cluster configuration.

Modem Configuration

Use this screen to access CC-SG from a client machine over a dial-up connection. This method of accessing CC-SG can be used in emergency situations.

Note: A modem is not available and cannot be configured on the V1 platform.

Configure CC-SG

1. On the **Setup** menu, click **Configuration Manager**. When the Configuration Manager screen appears, click on the **Modem** tab.



Figure 198 Configuration Manager Modem Screen

2. Type the **Server Address**, that is, the IP address of the CC-SG.
3. Type the **Client Address**, that is, the IP address of the client that will dial into CC-SG.
4. Type the **Client Phone**, that is, if using call-back dialing this is the call-back number that CC-SG dials to connect to the client.
5. Click **Update Configuration** to save the modem information to the system.
6. Click **Close** to close the Configuration Manager screen.

Configure the Modem on Client PC

Connect a phone line to the CC-SG, which has a built-in modem. Optionally, remove the LAN cables.

On the client that will be dialing in, connect a modem to the client machine, for example, a Windows XP machine. Connect a phone line to the client modem. Restart the client machine and the connected modem is discovered as new hardware. Install the modem on the client as follows, which assumes a Windows XP client machine:

1. Select **Control Panel** → **Phone and Modem Options**.
2. Click on the **Modems** tab.



Figure 199 Modems Tab

3. Click **Properties**.

- Click on the **Advanced** tab.

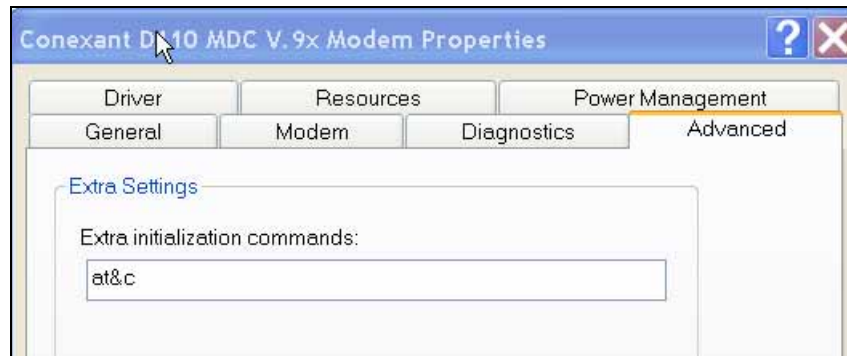


Figure 200 Extra Initialization Commands

- Type an initialization command in **Extra initialization commands** that will be used by your modem to set the “Carrier detection” flag. For example, type **at&c** for a SoftK56 Data Fax modem. This is necessary to tell Windows not to close the started Modem connection process when the modem connection is closed from the other (dialed-in) side. Click **OK** to save the settings.

Configure the Dial-Up Connection

The following procedure illustrates creating an inbound dial-up connection to CC-SG from a Windows XP client machine:

- On the **start** menu, click **My Network Places**.
- Right-click in the window and select **Properties**.
- Under **Network Tasks** in the **Network Connections** window, click **Create a new connection**.

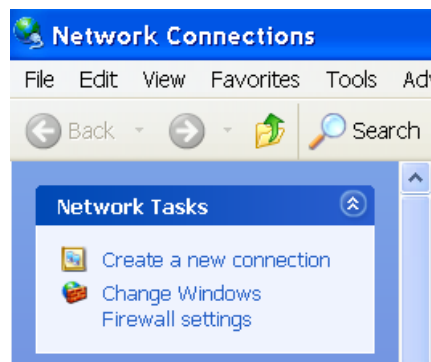


Figure 201 Create a new connection

- Click **Next**.



Figure 202 New Connection Wizard

- Click **Connect to the network at my workplace**.
- Click **Dial-up connection**.
- Type a name for CC-SG, for example **CommandCenter**.

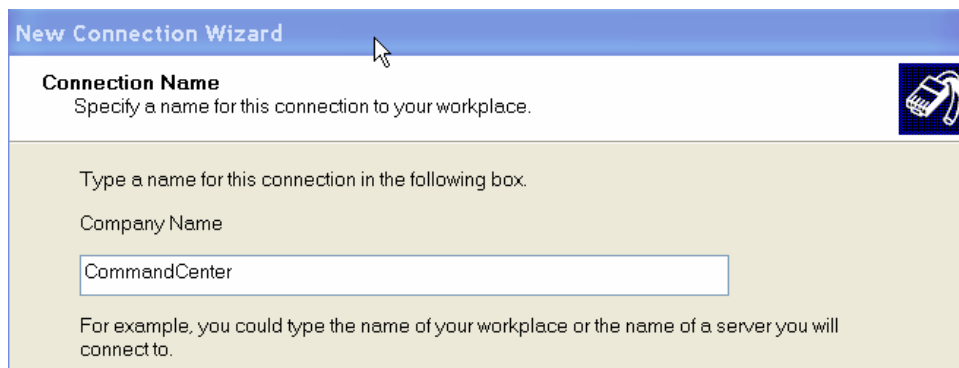


Figure 203 Connection Name

- Type the phone number used to connect to CC-SG and click **Next**. This is NOT the dial-back number that was configured as the **Client phone** under the **Modem** tab in **Configuration Manager** on CC-SG.

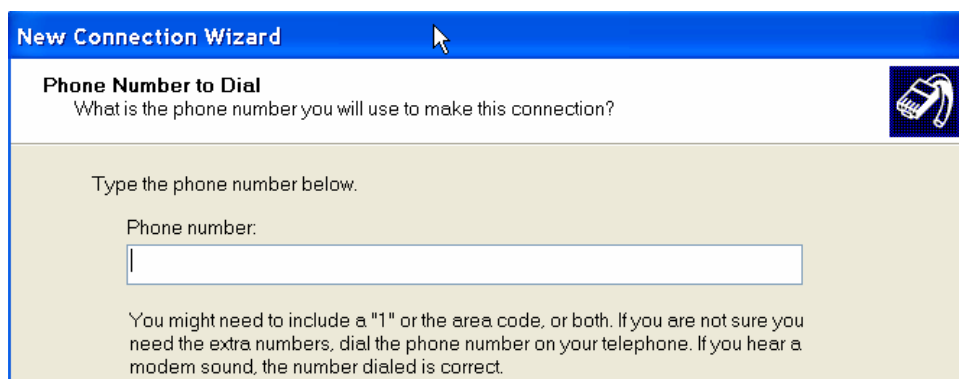


Figure 204 Phone Number to Dial

- A smart card is not necessary to dial into CC-SG. If you are not using one, click **Do not use my smart card** for this connection and click **Next**.

10. In the next screen, typically you want to click **My use only** in the next screen to make the connection available only to yourself.
11. Click **Finish** in the last screen to save the connection settings.

Configure the Call-back Connection

If the CC-SG uses a call-back connection, you need to use a script file that is described below. To supply the script file for call-back:

1. On the **start** menu, click **My Network Places**.
2. Click **view network connections** under **Network Tasks**.
3. Right-click on the **CommandCenter** connection and click **Properties**.
4. Click the **Security** tab.

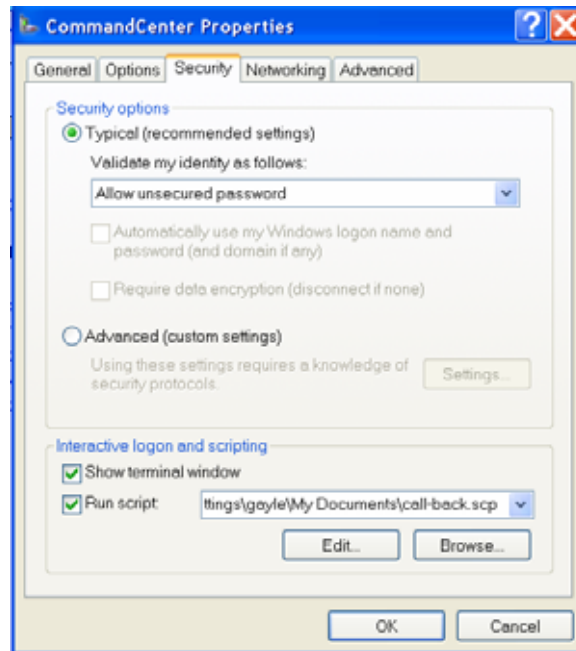


Figure 205 Specify Dial-up Script

5. Click the **Show terminal window**.
6. Click **Run script** and click **Browse** to enter the dial-up script, for example, **call-back.scp**.
7. Click **OK**.

Call-back Script File Example:

```
proc main
delay 1
waitfor "ogin:"
transmit "ccclient^M"
waitfor "client:"
transmit "dest^M"
waitfor "callback."
transmit "ATH^M"
waitfor "RING"
transmit "ATA^M"
waitfor "CONNECT"
waitfor "ogin:"
```

```
transmit "ccclient^M"  
endproc
```

Connect to CC-SG with Modem

To connect to CC-SG:

1. On the **start** menu, click **My Network Places**.
2. Click **view network connections** under **Network Tasks**.
3. Double-click on the **CommandCenter** connection.



Figure 206 Connecting to CC-SG

4. Type a username of **ccclient** and password of **cbupass**.



Figure 207 Entering username and password

5. If not filled in already, enter the phone number used to connect to CC-SG. This is NOT the dial-back number.
6. Click **Dial**. If using call-back, the modem will dial CC-SG and then CC-SG will dial your client PC.

7. If **Show terminal window** was checked as described in section **Configure the Call-back Connection** earlier in this chapter, then a window similar to the one below will be displayed:

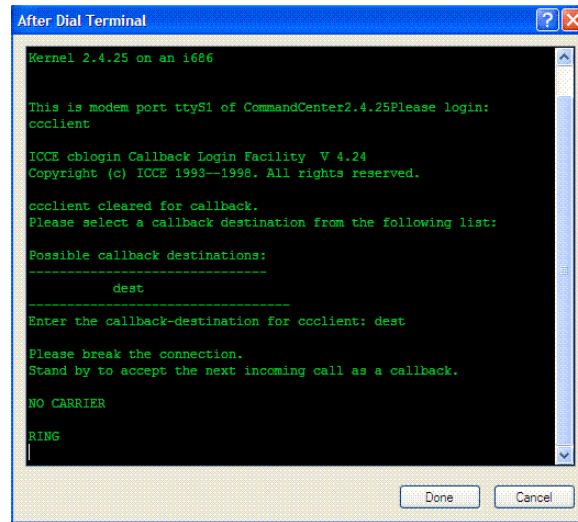


Figure 208 After Dial Terminal

8. Wait 1 or 2 minutes and in a supported browser, enter the IP address of CC-SG that was configured as the **Server address** under the **Modem** tab in **Configuration Manager** on CC-SG and login to CC-SG.

Connection Mode

When connected to a device, you have the option to pass data back and forth directly with that device (**Direct Mode**) or to route all the data through your CC-SG unit (**Proxy Mode**). While **Proxy Mode** increases the bandwidth load on your CC-SG server, you only need to keep the CC-SG TCP ports (80, 443, and 2400) open in your firewall. See Raritan's **Digital Solution Deployment Guide** for additional information.

1. On the **Setup** menu, click **Configuration Manager**. When the **Configuration Manager** screen appears, click on the **Connection Mode** tab.
2. Click on the radio button for the connection mode you prefer.
 - a. Click on the **Direct Mode** radio button to connect to a device directly.
 - b. Click on the **Proxy Mode** radio button to connect to a device via your CC-SG unit.

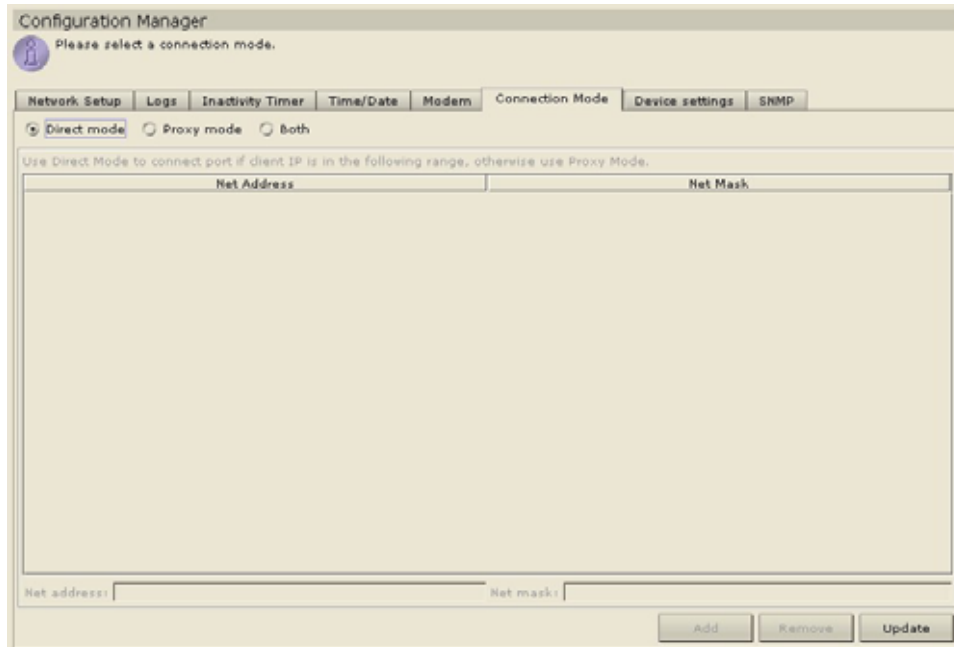


Figure 209 Configuration Manager Connection Screen – Direct Mode or Proxy Mode

- c. Click on the **Both** radio button if you want to connect to some devices directly, but others through **Proxy Mode**. Then specify settings for the devices you wish to connect to directly:
 - i. Type your client IP Address in the **Net Address** field at the base of the screen.
 - ii. Type your client net mask in the **Net Mask** field.

- iii. Click the **Add** button to add the Net Address and Mask to the screen. You may have to use the scroll bar on the right side of the screen to view the **Add/Remove/Update** buttons)

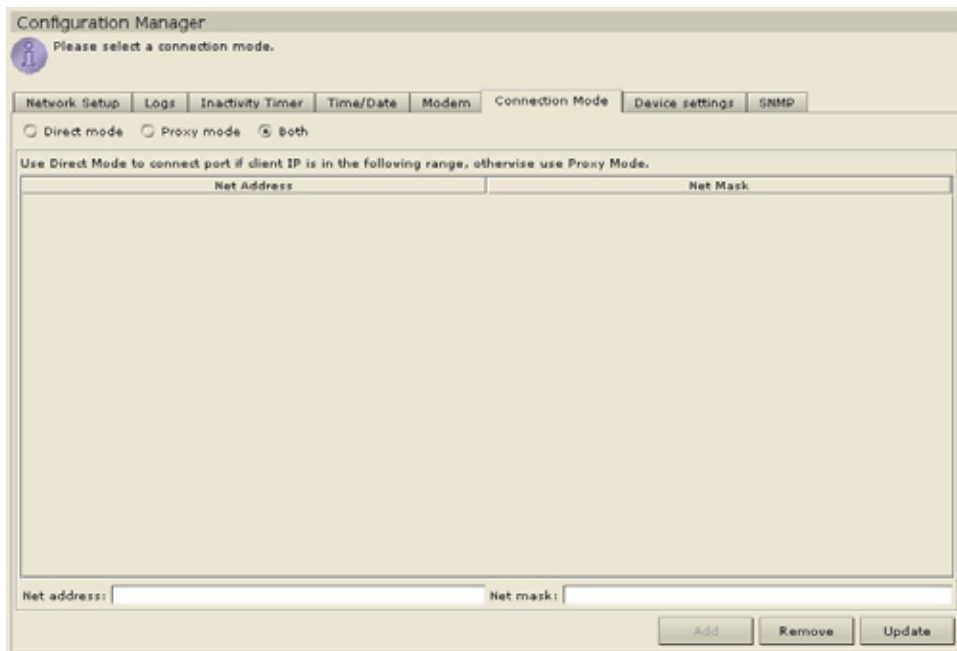


Figure 210 Configuration Manager Connection Screen – Both

Device Settings

1. On the **Setup** menu, click **Configuration Manager**. When the **Configuration Manager** screen appears, click on the **Device Settings** tab.
2. To update device Default Port, select a Device Type in the table and double-click on the Default Port value. Type the new Default Port value and press the **Enter** key.
3. To update device timeout duration, double-click on the Heartbeat (sec) value at the bottom of the screen. Type new timeout duration for this device.

Configuration Manager
Please provide devices default port and heartbeat information.

Network Setup | Logs | Inactivity Timer | Time/Date | Modem | Connection Mode | **Device settings** | SNMP

Device Type	Default Port
Domination KX	5000
IPMI Server	623
Domination KSK	5000
IP-Reach	5000
Domination KX101	5000
Domination SX	5000
Paragon II System Controller	5000

Heartbeat (sec): 600

Update Configuration

Close

Figure 211 Configuration Settings Device Settings Screen

4. Click **Update Configuration** to save the new device values. You may have to scroll down the screen to view the **Update** button. A success message will appear to confirm the update of all associated device settings.
5. Click **Close**.

SNMP

Simple Network Management Protocol allows CC-SG to push SNMP traps (event notifications) to an existing SNMP manager on the network. Only a CC-SG Administrator trained in handling an SNMP infrastructure should configure CC-SG to work with SNMP.

CC-SG also supports SNMP GET/SET operations with third-party enterprise Management Solutions, such as HP OpenView. To support the operations, you must provide SNMP agent identifier information such as these MIB-II System Group objects: sysContact, sysName, and sysLocation. Refer to RFC 1213 for details. These identifiers provide contact, administrative, and location information regarding the managed node.

MIB Files

Because CC-SG pushes its own set of Raritan traps, you must update all SNMP managers with a custom MIB file that contains Raritan SNMP trap definitions—see **Appendix E: SNMP Traps**. This custom MIB file can be found on the CD included with your CC-SG unit and also under **Firmware Upgrades** on <http://www.raritan.com/support>.

Configuring SNMP in CC-SG

1. On the **Setup** menu, click **Configuration Manager**. When the **Configuration Manager** screen appears, click on the **SNMP** tab.

The screenshot shows the 'SNMP' tab in the Configuration Manager. It is divided into three main sections: Agent Configuration, Traps Configuration, and Trap Destinations.

Agent Configuration: Includes fields for Version (2), IP Address (192.168.51.124), Port (161), Read-Only Community (public), Read-Write Community (private), System Desc (Raritan Computer; CommandCenter Secure Gateway; Version 3.0.1.1.1; G1 HW), System Contact, System Name, and System Location. An 'Update Agent Configuration' button is at the bottom right.

Traps Configuration: Features a checkbox for 'Enable SNMP Traps' (checked). Under 'Trap Sources', there are checkboxes for 'System Log' and 'Application Log' (both checked). A table lists trap sources with columns for 'Selected', 'Name', and 'Description':

Selected	Name	Description
☒	CCDeviceUpgrade	CC SecureGateway has upgraded the firmware on a ...
☒	CCImageUpgradeResults	CC SecureGateway Image Upgrade results

'Select All' and 'Clear All' buttons are to the right of the table.

Trap Destinations: A table lists destinations with columns for 'Host', 'Port', 'Version', and 'Community':

Host	Port	Version	Community
192.168.51.150	162	v2	public

Below the table are fields for 'Trap Destination Host', 'Port' (162), 'Community', and 'Version' (v1). 'Add' and 'Remove' buttons are to the right. An 'Update Trap Configuration' button is at the bottom right.

Figure 212 Configuration Settings Device Settings Screen

2. To identify the SNMP agent running on CC-SG to a third-party enterprise Management Solutions, provide agent information under **Agent Configuration**. Type a **Port** for the agent, default is **161**. Type a **Read-Only Community** string, default is **public**, and **Read-Write Community** string, default is **private**. Multiple community strings are allowed; separate them with a comma. Type a **System Contact**, **System Name**, and **System Location** to provide information regarding the managed node.
3. Click **Update Agent Configuration** to save the SNMP agent identifier information.
4. Under **Traps Configuration**, check the box marked **Enable SNMP Traps** to enable sending SNMP traps from CC-SG to a SNMP host.
5. Check the box(es) before the trap(s) you want CC-SG to push to your SNMP hosts:
Under **Trap Sources**, there is a list of SNMP traps grouped into two different categories:

System Log traps, which include notifications for the status of the CC unit itself, such as a hard disk failure, and **Application Log** traps for notifications generated by events in the CC application, such as modifications to a user account. To enable traps by type, check the boxes marked **System Log** and **Application Log**. Individual traps can be enabled or disabled by checking their corresponding checkboxes. Use **Select All** and **Clear All** to enable all traps or clear all checkboxes. Refer to the MIB files for the list of SNMP traps that are provided—see section **MIB Files**.

6. Type the **Trap Destination Host** IP address and **Port** number used by SNMP hosts in the **Trap Destinations** panel. Default port is 162.
7. Type the **Community** string and **Version** (v1 or v2) used by SNMP hosts in the **Trap Destinations** panel.
8. Click **Add** to add this destination host to the list of configured hosts. To remove a host from the list, select the host and click **Remove**. There is no limit to the number of managers that can be set in this list.
9. When SNMP traps and their destinations are configured, click **Update Trap Configuration**.

Configure Security

The General properties allow you to configure SSL for client connections, enable strong passwords, enable user lockout, and set the order of your authentication databases.

1. On the **Setup** menu, click **Security Manager**. When the **Security Manager** screen appears, click on the **General** tab.

Name	Type	Authentication	Authorization
AD92	AD	☒	☒
Local DB	DB	☒	☒
radius1	RADIUS	☐	☐
tacacs1	TACACS+	☐	☐
ldap2	LDAP	☐	☐
tacacs2	TACACS+	☐	☐
radius2	RADIUS	☐	☐
test Server	AD	☐	☐

CommandCenter Settings:

☐ Use SSL for client connections (requires restart)

☒ Force strong password check for the entire system and all users

SSH server port number: 22

Figure 213 Security Manager General Screen

2. Check the **Use SSL For Client Connections** check box if you want SSL encrypted connections to CC-SG. A restart of CC-SG is required after making a change.
3. Check the **Force strong password check for the entire system and all users** check box, if needed – see the next section. For strong passwords, minimum length is 6 characters and for non-strong passwords, minimum length is 4 characters.
4. Type the port number for accessing CC-SG via SSH. Please see **SSH Access to CC-SG**, later in this chapter, for additional information.
5. Click **Update** to update the changes.
6. Click **Close** to close the **Security Manager** screen.

Note: For information on the ordering of the authentication databases, please see **Chapter 9: Configuring Remote Authentication** for additional information.

Strong Password Rules

Strong password rules require users to observe strict guidelines when creating passwords, which makes the passwords more difficult to guess and, in theory, more secure. Administrators can enable or disable this feature — see the previous section **Configure Security**. When strong passwords are enabled, a password change will be rejected unless it meets the following criteria:

- Passwords must be at least six characters long.
- Passwords must contain at least one alphabetical character and one non-alphabetical character (number or punctuation symbol).
- The first four characters of the password and the username may not match.

Strong password rules apply only to user profiles stored locally. Password rules on an authentication server must be managed by the authentication server itself. Passwords stored on CC-SG should be managed by CC-SG and whatever rules it defines.

Enable User Lockout

Administrators can lock out CC-SG, CC-NOC users, and SSH users after a specified number of failed login attempts. This feature applies to users who are authenticated and authorized locally by CC-SG and does not apply to users who are remotely authenticated by external servers, see **Chapter 9: Configuring Remote Authentication** for additional information. Failed login attempts due to insufficient user licenses also do not apply.

Note: By default, the *ccroot* account is locked out for five minutes after three failed login attempts. For *ccroot*, the number of failed login attempts before lockout and after lockout is not configurable.

1. On the **Setup** menu, click **Security Manager**. When the **Security Manager** screen appears, click on the **General** tab.
2. Scroll down until you see **Lockout Settings**.

Figure 214 Lockout Settings

3. Click **Lockout Enabled**.
4. The default number of failed login attempts before a user is locked out is **3**. You can change this value by entering a number from **1** to **10**.
5. Choose a Lockout Strategy:
 - a. If you choose **Lockout for period** and specify a period of time, in minutes, the user will be locked out before they can login again. The default number is **5** minutes, but you can specify anywhere from **1** minute up to **1440** minutes (24 hours). After the time expires, the user can login again. At any time during the lockout period, an administrator can override this value and allow the user to log back into CC-SG.
 - b. If you choose **Lockout until admin allows access**, this means that users are locked out until an administrator allows them to log back in. To unlock a user, please see **Chapter 10: Generating Reports** for additional information.

6. Type an email address in **Lockout notification email** so notification is sent to the address informing the recipient that lockout has occurred. If the field is blank, notification is not sent.
7. Type a phone number in **Administrator's Phone** if the administrator needs to be contacted.
8. Click **Update** to save configuration settings.



Figure 215 Error (User Being Locked Out) Screen

Application Manager

Add Application

You can upload different custom applications to CC-SG and assign the applications to different ports in order to access them individually, as needed. Future application versions will be available on the Raritan website.

1. On the **Setup** menu, click **Application Manager**. The **Application Manager** screen appears.

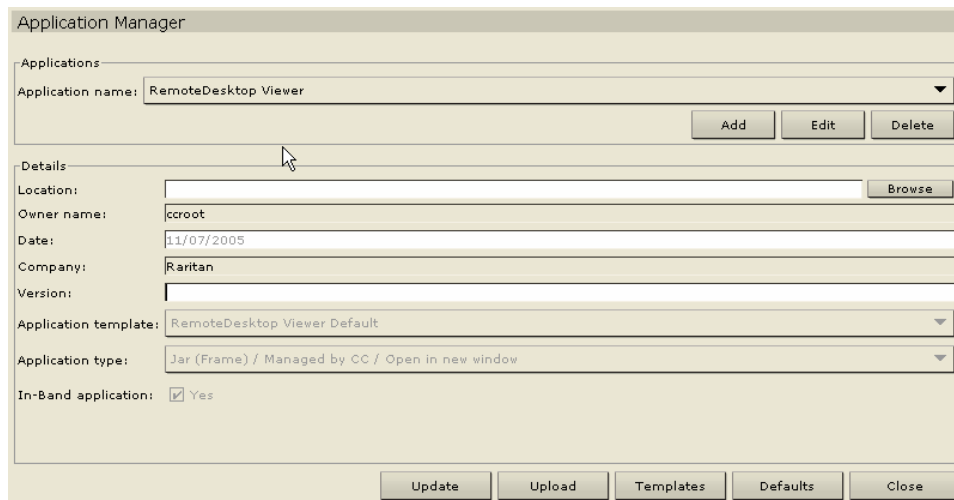


Figure 216 Application Manager Screen

2. Click **Add** to add a new application. The **Add Application** window appears.

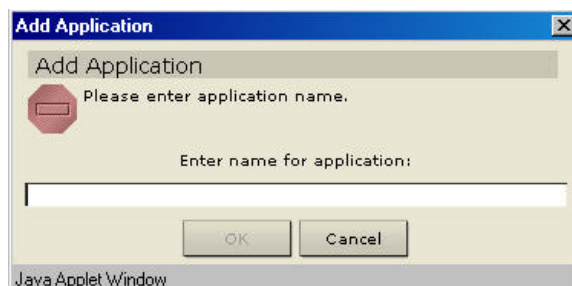


Figure 217 Add Application Window

3. Type the new application name in the **Enter Name for Application** field.

- Click **OK** to add the new application or **Cancel** to close the window. If you clicked **OK**, a search window appears.

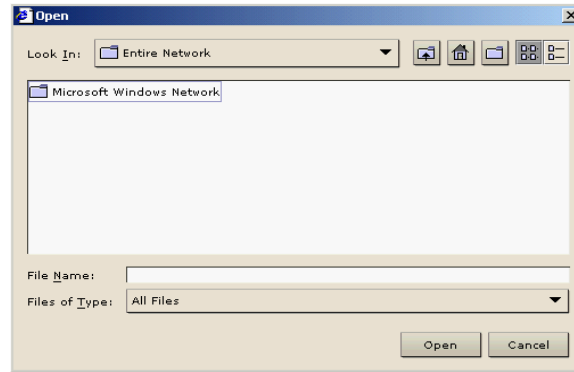


Figure 218 Search Window

- Click on the **Look In** drop-down arrow and navigate to locate the application in your system. When you find the application, select it, and click **Open**. The application name will appear in the **Location** field in the **Application Manager** screen.
- Click **Upload** to upload the application. A progress window indicates that the new application is being uploaded. When complete, a new window will indicate that the application has been added to the CC-SG database and is available for configuration and attachment to a specific port.
- Click **Close** to close the **Application Manager** screen.

Note: Once the application has been loaded into CC-SG and assigned to a port, verify that the application is operational.

Edit Application

Use this command to modify an application name or change the location where the application is stored in your system.

- On the **Setup** menu, click **Application Manager**. The **Application Manager** screen appears.
- Click on the **Application Name** drop-down arrow and select the application to be edited from the list.
- Click **Edit** in the **Applications** panel of the screen to rename the application. The **Edit Application** window appears.

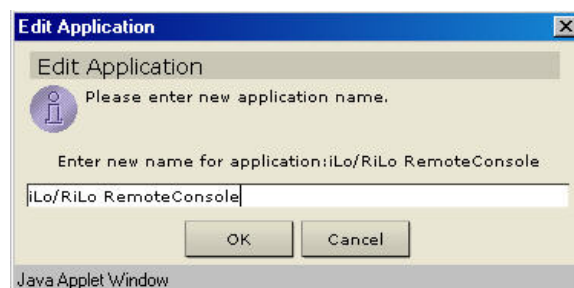


Figure 219 Edit Application Window

- Type the new application name in the **Enter New Name for Application** field.
- Click **OK** to edit the application name or **Cancel** to close the window.

6. Modify parameters in the **Parameters** panel and click the **Update** button in the **Details** panel of the screen. The parameters will be updated.
7. Click **Close** to close the **Application Manager** screen.

Delete Application

Deleting an application from the Application Manager removes it from the CC-SG database, although it is still retained in the local directory. When you delete a custom application, the serial port reverts to using RaritanConsole.

1. On the **Setup** menu, click **Application Manager**. The **Application Manager** screen appears.
2. Click on the **Application Name** drop-down arrow and select the application to be deleted.
3. Click the **Delete** button in the **Applications** panel to delete the application. The **Delete Application** window appears.

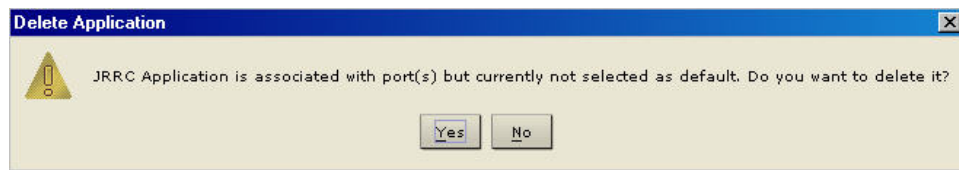


Figure 220 Delete Application Window

4. Click **Yes** to delete the application or **No** to close the window.
5. Click **Close** to close the **Application Manager** screen.

Firmware Manager

Upload Firmware

This command allows you to upload current versions of firmware to your system. Future firmware versions will be available on the Raritan website.

1. On the **Setup** menu, click **Firmware Manager**. The **Firmware Manager** screen appears.

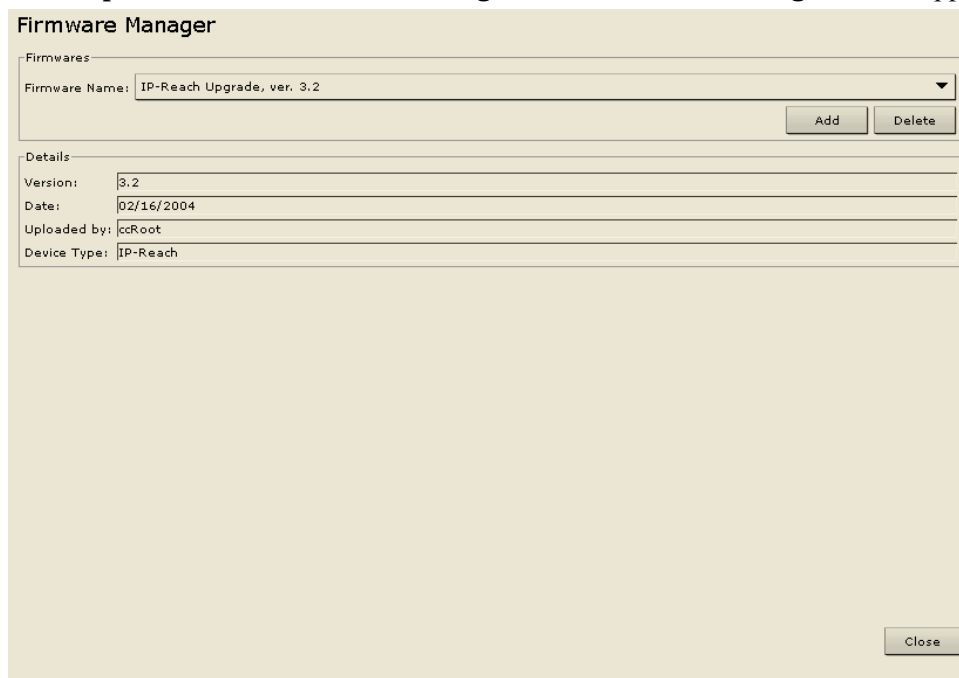


Figure 221 Firmware Manager Screen

- Click **Add** to add a new firmware file. A search window appears.

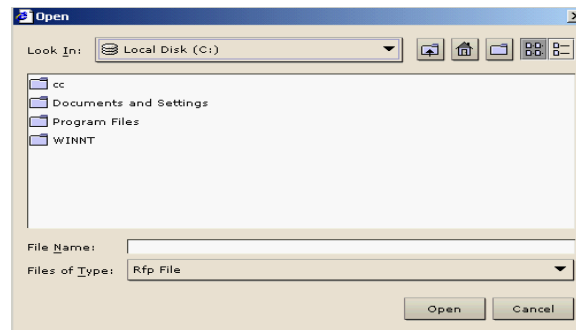


Figure 222 Search Window

- Click on the **Look In** drop-down arrow and navigate to locate the firmware file in your system. When you find the firmware, select it, and click **Open**. The firmware name will appear in the **Firmware Name** field.
- Click **Close** to close the **Firmware Manager** screen.

Delete Firmware

- On the **Setup** menu, click **Firmware Manager**. The **Firmware Manager** screen appears.
- Click on the **Firmware Name** drop-down arrow and select the firmware to be deleted.
- Click **Delete**. The **Delete Firmware** window appears.

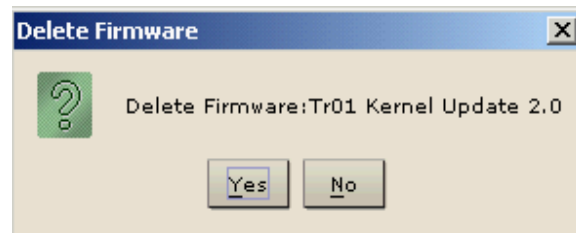


Figure 223 Delete Firmware Window

- Click **Yes** to delete the firmware or **No** to close the window.
- Click **Close** to close the **Firmware Manager** screen.

CommandCenter NOC

Adding a CommandCenter NOC (CC-NOC) to your setup will expand your target management capabilities by providing monitoring, reporting, and alert services for your serial and KVM target systems. Please see Raritan's *CommandCenter NOC* documentation for detailed instructions on installing and operating your CC-NOC appliance.

Important: In the following procedure, passcodes are generated. You need to provide these passcodes to the CC-NOC administrator who needs to configure them in CC-NOC within five minutes. Avoid transmitting the passcodes over email or other electronic means to avoid a possible interception by automated systems. A phone call or exchange of written codes between trusted parties is better protection against automated interception.

Add a CC-NOC

Note: To create a valid connection, the time settings on both the CC-NOC and CC-SG should be synchronized. The best method of achieving this synchronization, it to use a common NTP (Network Time Protocol) server. For this reason, the CC-NOC and CC-SG are required to be configured to use an NTP server.

1. On the **CommandCenter NOC** menu, click **Configuration**. The **CC-NOC Configuration** screen appears.

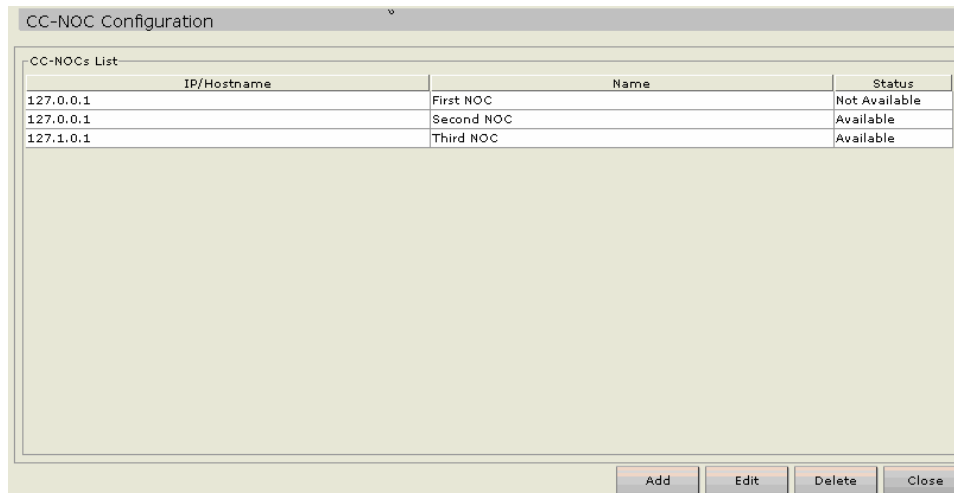


Figure 224 CC-NOC Configuration Screen

2. Click **Add**. The **Add CC-NOC Configuration** screen appears.

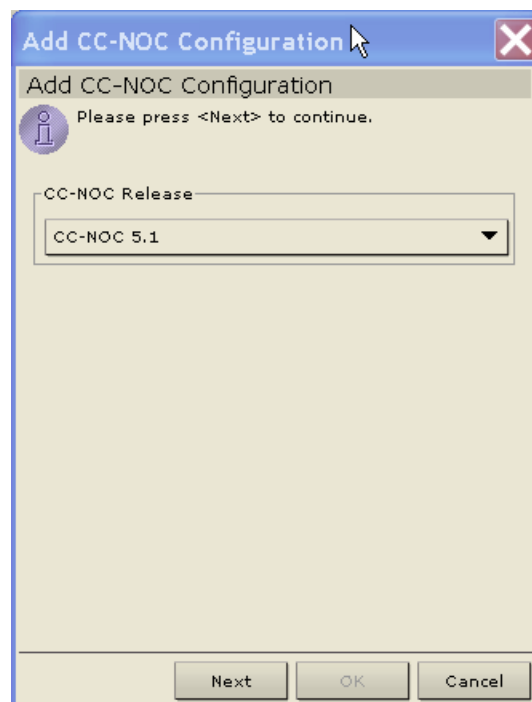


Figure 225 CC-NOC Configuration Screen

3. Select a software version of CC-NOC you want to add and click **Next**. Version 5.1 has fewer integration features than 5.2 and only requires adding a name and an IP address. For additional information on CC-NOC 5.1, please see www.raritan.com/support. Click on **Product Documentation**, then **CommandCenter NOC**.

Figure 226 Add CC-NOC Configuration Screen

4. Type a descriptive name of the CC-NOC in the **Name** field. Maximum length is 50 alphanumeric characters.
5. Type the IP address or hostname of the CC-NOC in the **CC-NOC IP/Hostname** field. This is a required field. For hostname rules, see **Terminology/Acronyms** in **Chapter 1: Introduction**.
6. To retrieve daily information on targets in the CC-NOC database, type a discovery range in the **IP Range From** and **IP Range To** fields. This IP range represents the range of addresses CC-SG is interested in and instructs CC-NOC to send events for these devices to CC-SG. This range is related to the discovery range that is configured in the CC-NOC—see Raritan’s **CommandCenter NOC Administrator Guide** for details. Type a range, keeping the following rules in mind:

IP ADDRESS RANGE	DESCRIPTION
If CC-SG range entered here is a <i>subset</i> of the range configured in CC-NOC...	... then , CC-NOC returns all known target device information within this range.
If CC-SG range entered here includes a <i>partial</i> list (non-null intersection) of the range configured in CC-NOC...	... then , CC-NOC returns all known target device information within the intersecting range.
If CC-SG range is a <i>superset</i> of the range configured in CC-NOC...	... then , CC-NOC returns all known target device information within this range. Essentially, CC-NOC returns targets that are defined in the CC-NOC range.
If CC-SG range does not <i>overlap</i> the range configured in CC-NOC...	... then , CC-NOC will not return any target device information at all.

To stop CC-NOC from monitoring a device, it can be *unmanaged* – see the **CommandCenter NOC Administrator Guide**.

Note: Use the CC-NOC Synchronization Report to view targets that the CC-SG is subscribing to. The report also displays any new targets that have been discovered by CC-NOC. See Chapter 10: Generating Reports, CC-NOC Synchronization Report for additional information.

7. Specify a **Synchronization Time** to schedule when the target information is retrieved from the CC-NOC database. This will refresh the databases as targets are discovered or become unmanaged. The default is the current time as set on the client machine. You may want to schedule synchronization during an off-peak time so synchronization will not affect the performance of other processes.
8. For **Heartbeat Interval**, enter how often, in seconds, CC-SG sends a heartbeat message to CC-NOC. This confirms if CC-NOC is still up and available. Default is **60** seconds. Valid range is **30-120** seconds. Normally, this does not have to be changed.
9. For **Failed Heartbeat Attempts**, enter the number of consecutive heartbeats that must pass without a response before a CC-NOC node is considered unavailable. Default is **2** heartbeats. Valid range is **2-4** heartbeats. Normally, this does not have to be changed.
10. Click **Next**.

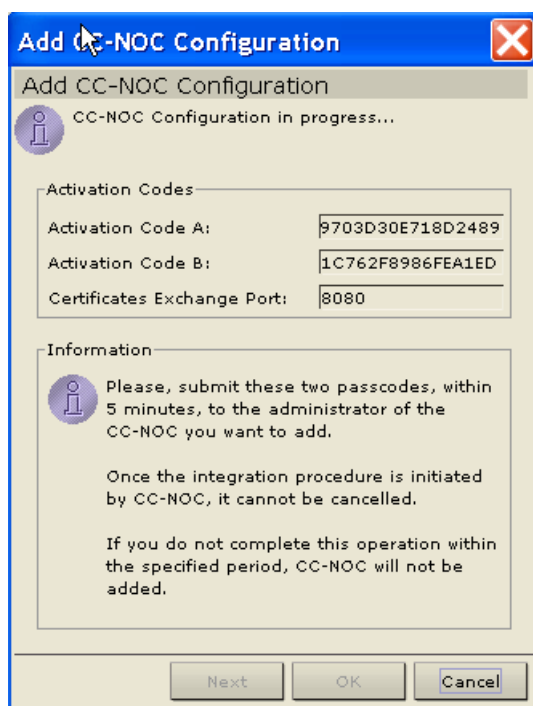


Figure 227 CC-NOC Passcodes

11. Either copy and paste the passcodes into CC-NOC fields if you are the CC-NOC administrator or submit the two passcodes to the CC-NOC administrator. As documented in the **CommandCenter NOC Administrator Guide**, the CC-NOC administrator will then enter the passcodes in CC-NOC, which initiates an exchange of security certificates.

Important: To increase security, you must enter the passcodes in CC-NOC within five minutes after they are generated on CC-SG. This will minimize the window of opportunity for intruders to breach the system with a brute-force attack. Avoid transmitting the passcodes over email or other electronic means to avoid a possible interception by automated systems. A phone call or exchange of written codes between trusted parties is better protection against automated interception.

12. Once the certificate exchange process is complete, a secure channel has been established between CC-NOC and CC-SG. The CC-NOC data will be copied to CC-SG. Click **OK** to complete the process. If the process does not complete within 5 minutes, it times out and data is not saved in CC-SG and any stored certificates are deleted. Retry the procedure again—go to Step 1. in **Add a CC-NOC** on page 182.

Note: *CommandCenter NOC can only be added to standalone or primary node CC-SG servers.*

Edit a CC-NOC

1. On the **CommandCenter NOC** menu, click **Configuration**. The **NOC Configuration** screen appears.

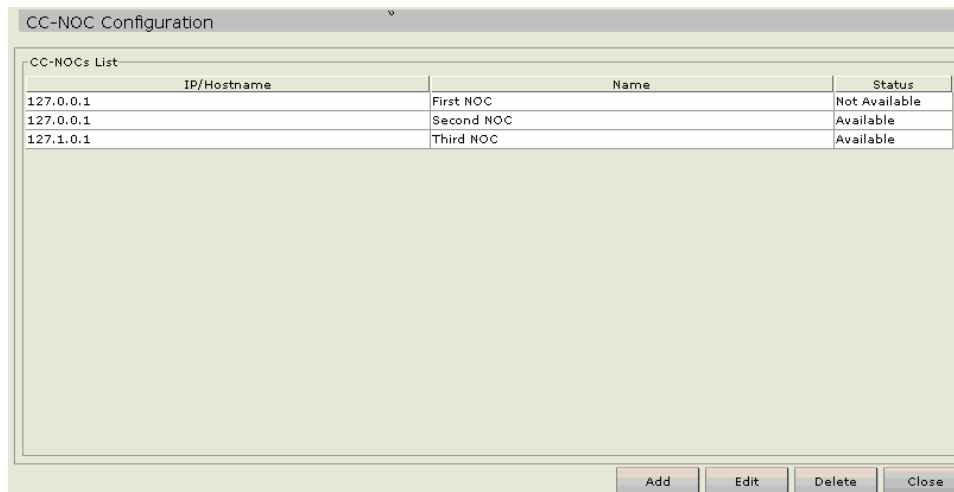
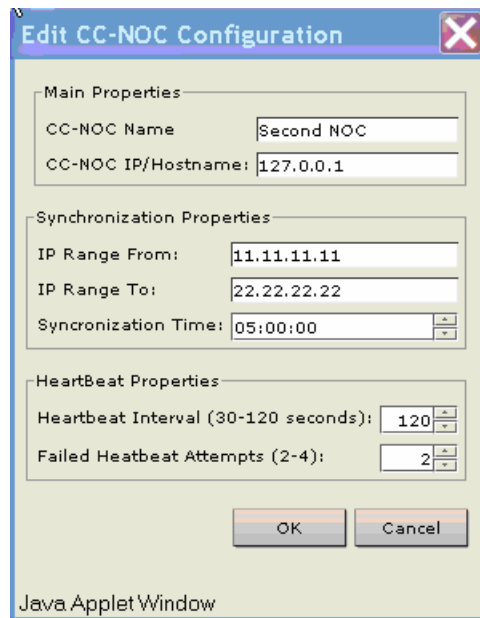


Figure 228 CC-NOC Configuration Screen

- Highlight a CC-NOC in the list and click **Edit**. The **Edit CC-NOC Configuration** screen appears.



The **Edit CC-NOC Configuration** screen is a Java Applet Window with a title bar and a close button. It contains three sections of configuration fields:

- Main Properties:**
 - CC-NOC Name:
 - CC-NOC IP/Hostname:
- Synchronization Properties:**
 - IP Range From:
 - IP Range To:
 - Synchronization Time:
- HeartBeat Properties:**
 - Heartbeat Interval (30-120 seconds):
 - Failed Heartbeat Attempts (2-4):

At the bottom are **OK** and **Cancel** buttons. The text "Java Applet Window" is at the bottom left.

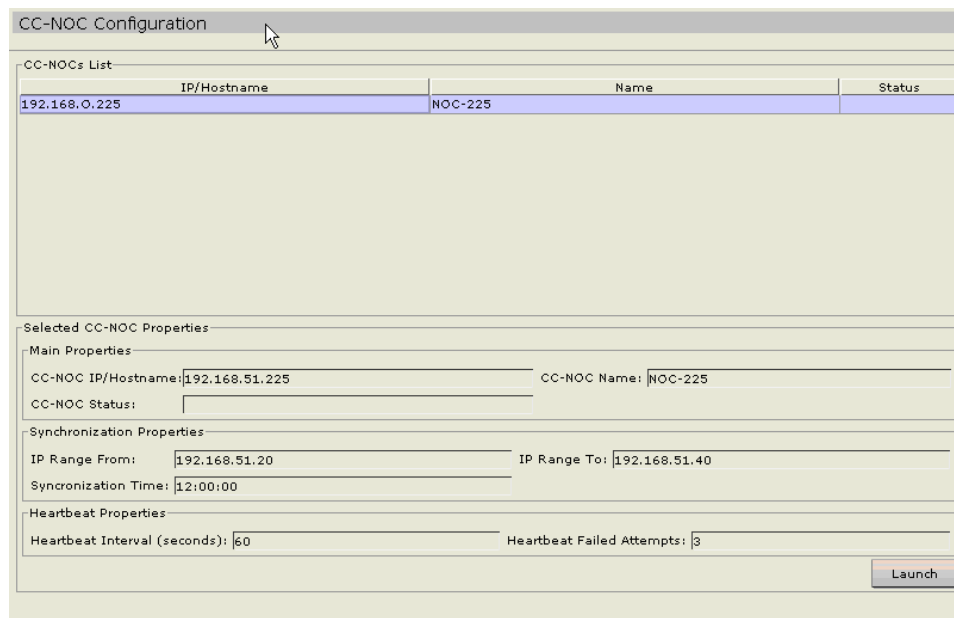
Figure 229 Edit CC-NOC Configuration Screen

- Refer to the previous section **Add a CC-NOC** for field details.

Launch CC-NOC

To launch CC-NOC from CC-SG:

- In the CC-NOC Configuration screen, highlight an available CC-NOC.
- Click **Launch**. This will connect you to a configured CC-NOC.



The **CC-NOC Configuration** screen displays a table of CC-NOCs and a section for selected properties.

IP/Hostname	Name	Status
192.168.0.225	NOC-225	

Selected CC-NOC Properties:

- Main Properties:**
 - CC-NOC IP/Hostname:
 - CC-NOC Name:
 - CC-NOC Status:
- Synchronization Properties:**
 - IP Range From:
 - IP Range To:
 - Synchronization Time:
- Heartbeat Properties:**
 - Heartbeat Interval (seconds):
 - Heartbeat Failed Attempts:

A **Launch** button is located at the bottom right.

Figure 230 Launch CC-NOC

Delete a CC-NOC

To remove and unregister a CC-NOC in CC-SG, do the following.

1. On the **CommandCenter NOC** menu, click **Configuration**. The **CC-NOC Configuration** screen appears.

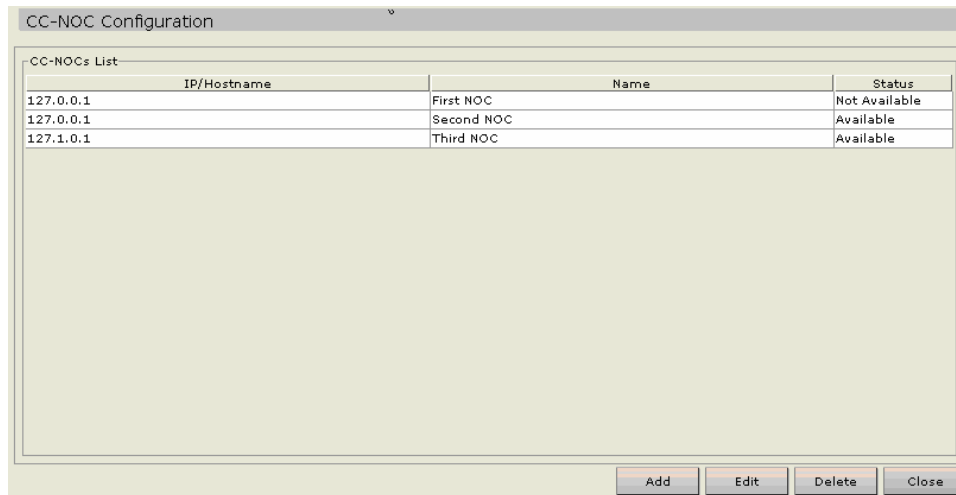


Figure 231 Delete CC-NOC Screen

2. Highlight a CC-NOC in the list and click **Delete**. You are prompted to confirm the deletion.
3. Click **Yes** to delete the CC-NOC or **No** to exit without deleting. A **CC-NOC Deleted Successfully** message confirms that CC-NOC has been deleted.
4. Repeat steps 1 through 3 to delete other CC-NOCs.

Cluster Configuration

A CC-SG cluster uses two CC-SG nodes, one Primary node and one Secondary node, for backup security in case of Primary CC-SG node failure. Both nodes share common data for active users and active connections, and all status data is replicated between the two nodes. The primary and secondary nodes in a cluster must be running the same version of software. Unless defined by the user, CC-SG will assign a default name to each cluster node.

Devices in a CC-SG cluster must be aware of the IP of the Primary CC-SG node in order to be able to notify the Primary node of status change events. If the Primary node fails, the Secondary node immediately assumes all Primary node functionality. This requires initialization of the CC-SG application and user sessions and all existing sessions originating on the Primary CC-SG node will terminate. The devices connected to the Primary CC-SG unit will recognize that the Primary node is not responding and will respond to requests initiated by the Secondary node.

Note: In a cluster configuration, only the Primary CC-SG communicates with CC-NOC. Whenever a CC-SG becomes primary, it sends its IP address, in addition to the IP address of the Secondary CC-SG, to CC- NOC.

Create a Cluster

In the event of a failover, the administrator should send an email to all CC-SG users, notifying them to use the IP address of the “new” Primary CC-SG node.

Important: It is recommended to backup your configuration on both nodes before setting up a cluster configuration.

Set Primary CC-SG Node

1. On the **Setup** menu, click **Cluster Configuration**. The Cluster Configuration screen appears.
2. Click **Discover CommandCenters** to scan and display all CC-SG appliances on the same subnet as your one you are currently using. Alternatively, you can add a CC-SG, perhaps from a different subnet, by specifying an IP address in **CommandCenter address** in the bottom of the window. Click **Add CommandCenter**.

Cluster Configuration

This CommandCenter is not a member of any cluster.

Cluster Name	Node Address	Node State	CommandCenter version
	192.168.51.124	Standalone	3.0.0.1.10
	192.168.51.102	Standalone	3.0.0.1.7
	192.168.51.201	Standalone	2.3.0.5.3
	192.168.51.74	Standalone	3.0.0.1.8
cc_rak_4	192.168.51.66	Primary	3.0.0.1.7
	192.168.51.218	Standalone	2.20.5.1
	192.168.51.238	Standalone	2.20.5.1
	192.168.51.150	Standalone	2.21.5.1

Cluster Management

CommandCenter address:

Cluster Name:

Backup username: Password:

Figure 232 Cluster Configuration Screen

3. Type a name for this cluster in **Cluster Name**. If you do not provide a name now, a default name will be provided, such as **cluster192.168.51.124**, when the cluster is created.
4. Click **Create Cluster**.
5. Click **Yes** when prompted if you want to continue. The CC-SG you currently are using will become the Primary node and a default name will be provided unless you previously entered one.

Cluster Configuration

This CommandCenter is a member of cluster: cluster192.168.51.124

Cluster Name	Node Address	Node State	CommandCenter version
	192.168.51.102	Standalone	3.0.0.1.7
	192.168.51.201	Standalone	2.3.0.5.3
	192.168.51.74	Standalone	3.0.0.1.8
cc_rak_4	192.168.51.66	Primary	3.0.0.1.7
	192.168.51.218	Standalone	2.20.5.1
	192.168.51.238	Standalone	2.20.5.1
	192.168.51.150	Standalone	2.21.5.1
cluster192.168.51.124	192.168.51.124	Primary	3.0.0.1.10

Figure 233 Cluster Configuration – Primary Node Set

Set Secondary CC-SG Node

1. Click **Discover CommandCenters** to scan and display all CC-SG appliances on the same subnet as your one you are currently using. Alternatively, you can add a CC-SG, perhaps from a different subnet, by specifying an IP address in **CommandCenter address** in the bottom of the window. Click **Add CommandCenter**.

Note: Adding a backup CC-SG from a different subnet or network may avoid issues affecting a single network or physical location.

2. To add a Secondary Node, or backup CC-SG node, select a CC-SG unit with **Standalone** status from the Cluster Configuration table. The version number must match the primary node's version.
3. Type a valid user name and password for the backup node.

The screenshot shows the 'Cluster Configuration' window. At the top, it states 'This CommandCenter@ is a member of cluster: CCSG_Cluster_Test'. Below this is a table with four columns: Cluster Name, Node Address, Node State, and CommandCenter@ version. The table contains four rows of data. The first row is highlighted in blue. Below the table is a 'Cluster Management' section with input fields for 'CommandCenter@ address:', 'Cluster Name:', 'Backup username:', and 'Password:'. There are buttons for 'Add CommandCenter@', 'Discover CommandCenter@', 'Remove Cluster', 'Join "Backup" Node', 'Advanced', and 'Close'.

Cluster Name	Node Address	Node State	CommandCenter@ version
CCSG_Cluster_Test	192.168.32.58	Primary	2.3.0.1.6
	192.168.32.11	Standalone	2.20.5.1
	192.168.32.34	Standalone	2.21.5.1
	192.168.51.131	Standalone	2.3.0.1.6

Cluster Management

CommandCenter@ address: Add CommandCenter@ Discover CommandCenter@

Cluster Name:

Backup username: Password:

Remove Cluster Join "Backup" Node Advanced Close

Figure 234 Cluster Configuration – Set Secondary CC-SG

4. Click **Join "Backup" Node**.
5. A confirmation message will appear. Click **Yes** to assign Secondary status to the selected node, or click **No** to cancel.
6. After you click **Yes**, CC-SG will restart the newly selected Secondary node. This process can take several minutes. When restart is complete, a confirmation message appears on your screen.
7. On the **Setup** menu, click **Cluster Configuration** to view the updated Cluster Configuration table.

Note: If the Primary and Secondary Nodes lose communication with one another, the Secondary Node will assume the role of the Primary Node. When connectivity resumes, you may have two Primary Nodes. You should then remove a Primary Node and reset it as a Secondary Node.

Remove Secondary CC-SG Node

1. To remove Secondary Node status from a CC-SG unit and reassign it to a different unit in your configuration, select the Secondary CC-SG Node in the Cluster Configuration table and click **Remove “Backup” Node**.
2. When the confirmation message appears, click **Yes** to remove Secondary Node status, or click **No** to cancel.

Note: Clicking **Remove “Backup” Node** does not delete the Secondary CC-SG unit from your configuration; it simply removes the designation of Secondary Node.

Remove Primary CC-SG Node

1. To remove Primary Node status from a CC-SG unit and reassign it to another unit in your configuration, select the Primary CC-SG Node in the Cluster Configuration table and click **Remove Cluster**.
2. When the confirmation message appears, click **Yes** to remove Primary Node status, or click **No** to cancel.

Note: Clicking **Remove Cluster** does not delete the Primary CC-SG unit from your configuration; it simply removes the designation of Primary Node. **Remove Cluster** is only available when no backup nodes exist.

3. Click **Close** to exit the Cluster Configuration screen.

Recover a Failed CC-SG Node

When a node fails and failover occurs, the failed node will recover in **Waiting** status.

1. Select the Waiting node in the Cluster Configuration table.
2. Add it as a backup node by clicking **Join “Waiting” Node**.
3. A confirmation message will appear. Click **Yes** to assign Secondary status to the selected node, or click **No** to cancel. If you click **Yes**, you will need to wait for the secondary node to restart just as with **Join “Backup” Node**.

Note: Once a node is in **Waiting** status it can be started in **Standalone** mode or **Backup** mode.

Cluster Configuration

This CommandCenter is a member of cluster: cluster192.168.51.97

Cluster Name	Node Address	Node State	CommandCenter version
cluster192.168.51.97	192.168.51.97	Primary	2.20.1.17
cluster192.168.51.97	192.168.52.62	Waiting	2.20.1.17

Cluster Management

CommandCenter address:

Cluster Name:

Backup username: Password:

Figure 235 Recovering a node from Waiting status

Set Advanced Settings

To configure advanced settings of a cluster configuration:

1. Select the Primary node just created.
2. Click **Advanced**. The **Advanced Settings** window appears.

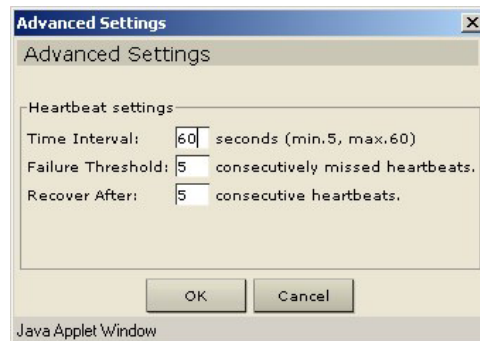


Figure 236 Cluster Configuration Advanced Settings

3. For **Time Interval**, enter how often CC-SG should check its connection with the other node.

Note: Setting a low Time Interval will increase the network traffic generated by heartbeat checks. Also, clusters with nodes located far apart from each other may want to set higher intervals.

4. For **Failure Threshold**, enter the number of consecutive heartbeats that must pass without a response before a CC-SG node is considered failed.
5. For **Recover After**, enter the number of consecutive heartbeats that must successfully be returned before a failed connection is considered recovered.
6. Click **OK** to save the settings or **Cancel** to exit without saving.

Note: Changing the time zone is disabled in a cluster configuration.

Task Manager

Use Task Manager to schedule CC-SG tasks on a daily, weekly, monthly, or yearly basis. A task can be scheduled to run only once or periodically on a specified day of the week and at a specified interval, such as, scheduling device backups every three weeks on Fridays or emailing a particular every Monday to one or more recipients.

Note: Tasks use the Server time that is set on CC-SG for scheduling and not the time on your client PC.

Task Types

These tasks can be scheduled:

- Backup Device Configuration (individual device or device group)
- Restore Device Configuration (does not apply to device groups)
- Copy Device Configuration (individual device or device group)
- Upgrade Device Firmware (individual device or device group). Note that the firmware should be made available before scheduling this task.
- Backup Command Center Secure Gateway
- Restart Device (does not apply to device groups)

- Outlet Port Power Management (Power On/Off/Recycle Outlet ports)
- Generate all Reports (HTML or CSV formats)
- Purge Logs

Scheduling Sequential Tasks

You may want to schedule tasks sequentially to confirm that expected behavior was actually carried out. For example, you may want to schedule an Upgrade Device Firmware task for a given device group and then schedule generating an Asset Management Report task immediately after it to confirm that the correct versions of firmware were upgraded.

Email Notifications

Upon completion of a task, an email message can be sent to a specified recipient. How the email is sent, such as if it is sent securely via SSL, is configured in the Notification Manager (please see **Notification Manager**, later in this chapter, for additional information).

Stored Reports

Reports that are scheduled are sent via email to the recipients that are specified.

All reports that have a **Finished** status are stored on CC-SG for 30 days and can be viewed by selecting **View Stored Reports** under the **Reports** menu. Please see **Chapter 10: Generating Reports, View Stored Reports** for additional information.

Create a New Task

To schedule a new task:

1. On the **Setup** menu, click **Task Manager**.

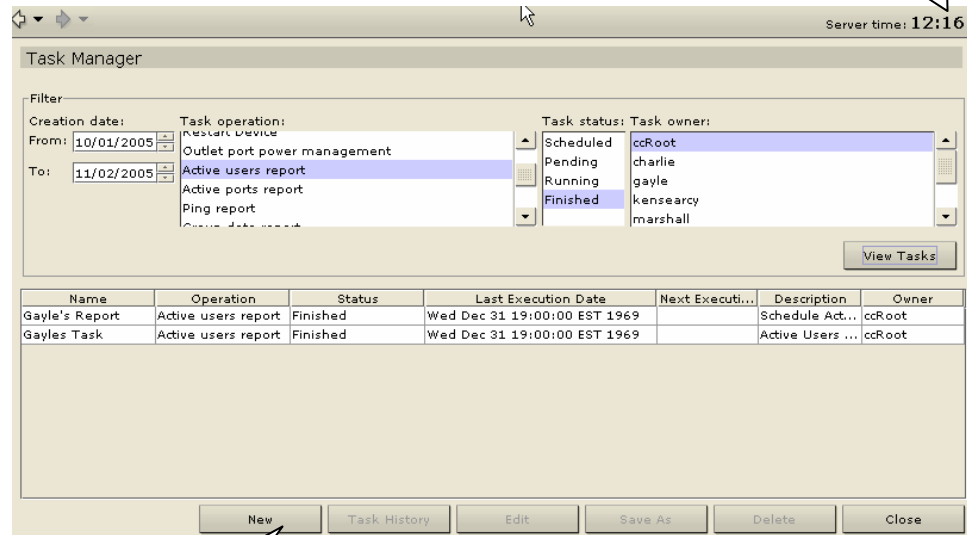


Figure 237 Task Manager

2. Click **New**.

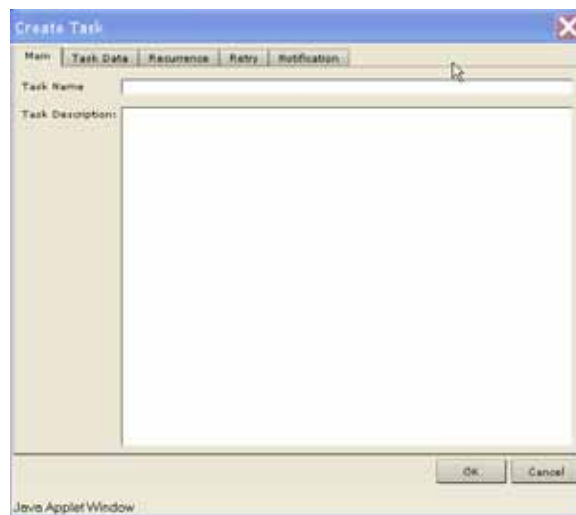


Figure 238 Create Task

3. In the **Main** tab, type a name (1-32 characters, alphanumeric characters or underscores, no spaces) and description for the task.

- Click on the **Task Data** tab and from the pulldown menu, select the task to be scheduled, such as **Upgrade Device Firmware**. Note that the fields requiring data will vary according to the task selected. With the exception of **Restart Device** and **Restore Device**, a single device or devices in a group can be selected for tasks involving devices.

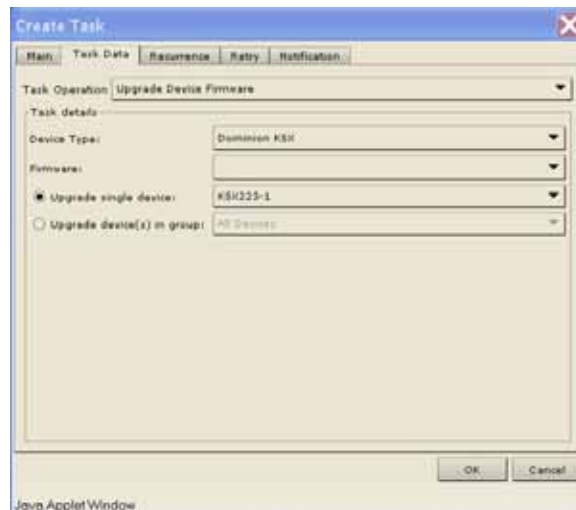


Figure 239 Selecting a Task to Schedule

Note: If filtering on fields of scheduled reports, please see Chapter 10: Generating Reports for additional information.

- Click on the **Recurrence** tab and select a **Period** (once, periodic, daily, weekly, monthly, yearly). For periods that do include an initial starting time, for example, **Weekly**, enter a **Start at** time (based on the CC-SG server time as displayed near the top of the main window), **Start date** and **End date** in **Range of recurrence**.

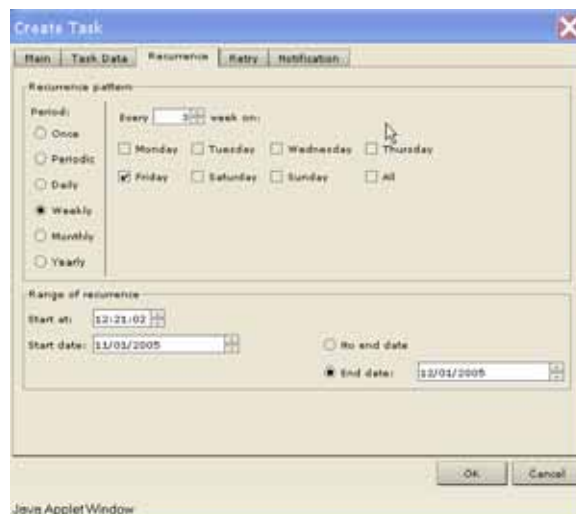


Figure 240 Specifying Task Recurrence

- Click on the **Retry** tab to reset values for **Retry Count** and **Retry Interval**. Select the unit for time (seconds, minutes, hours, or days). Default is 3 and 5 respectively. **Retry Count** specifies the number of times the task is attempted to execute if it fails and **Retry Interval** is the amount of time between attempts.
- Click on the **Notification** tab to specify email recipients. By default, the email address of the user currently logged in will be used. The user's email is configured in the user profile—see section

8. **Change Own Password** in **Chapter 7: Adding Users and User Groups**. If an email was not configured, then this field is blank. By default, email is sent if the task was successful. To notify the recipient of failed tasks, click the **On Failure** checkbox.

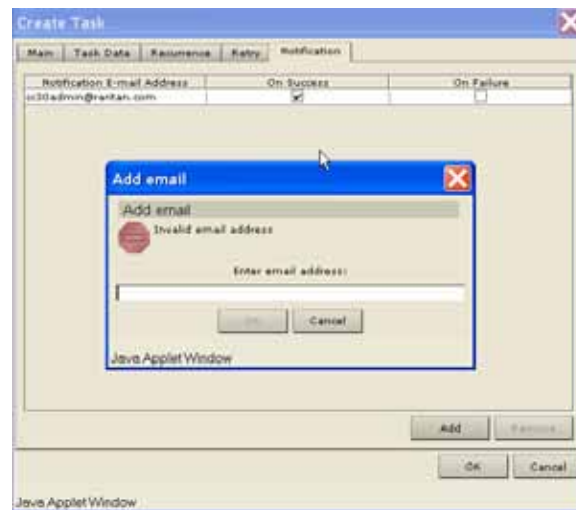


Figure 241 Specifying Task Email Notification

9. To send email to additional recipients, click **Add**. Enter a valid email address and click **OK**. Then click **On Success** to have the recipient be notified if the task was successful or **On Failure** to have the recipient be notified if the task failed or both.

View a Task, Details of a Task, and Task History

To view a task:

1. On the **Setup** menu, click **Task Manager**.

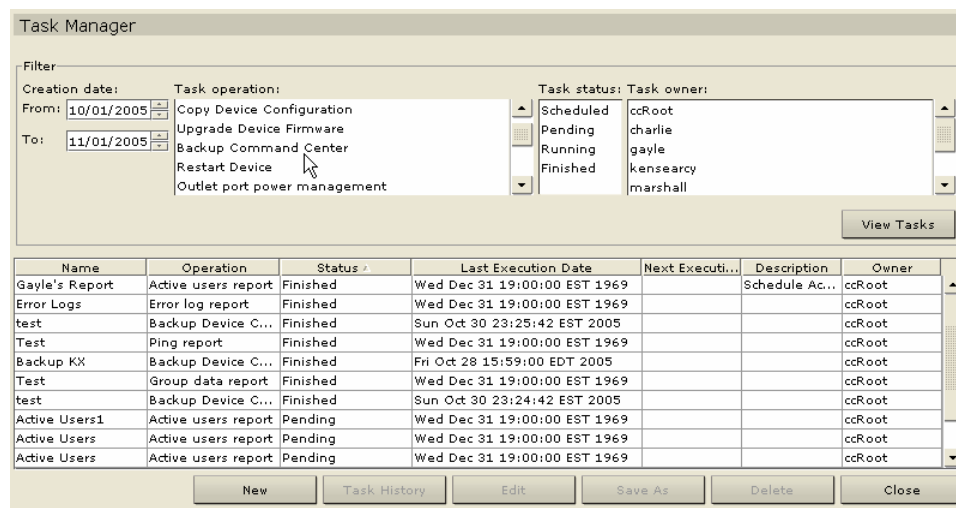
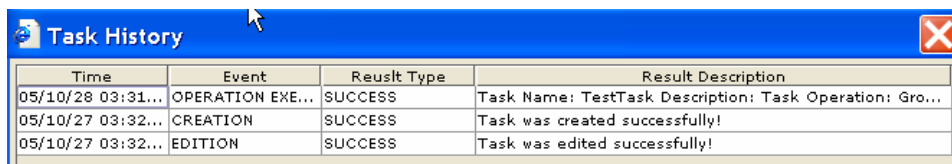


Figure 242 View a Task

2. Click **View Tasks** to view the entire list of tasks created by all owners and with all statuses. By default, all tasks that were created a month ago to today's date are displayed.
3. To filter the tasks displayed, you can alter the date by highlighting the month, date, or year fields and clicking the or buttons. You can filter the list further by selecting one or more (**Ctrl+click**) tasks, status, or owner. Click **View Tasks** to view the filtered list.

Note: You cannot delete a task that is currently running.

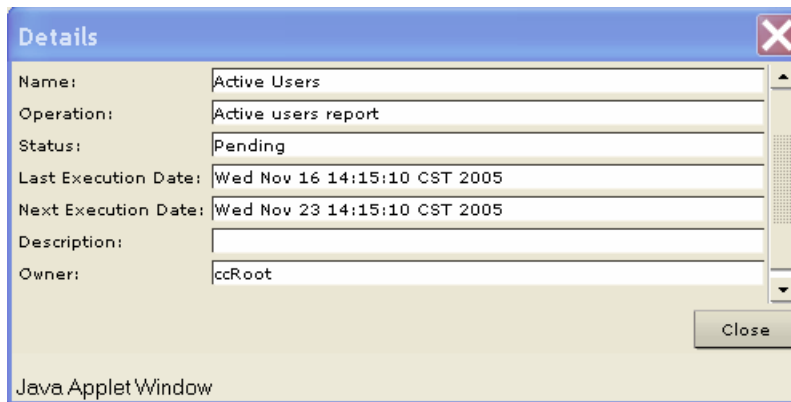
4. To view the history of a task, select a task and click **Task History**.



Time	Event	Result Type	Result Description
05/10/28 03:31...	OPERATION EXE...	SUCCESS	Task Name: TestTask Description: Task Operation: Gro...
05/10/27 03:32...	CREATION	SUCCESS	Task was created successfully!
05/10/27 03:32...	EDITION	SUCCESS	Task was edited successfully!

Figure 243 Task History

5. To view details of a task, double-click on a task.



Details	
Name:	Active Users
Operation:	Active users report
Status:	Pending
Last Execution Date:	Wed Nov 16 14:15:10 CST 2005
Next Execution Date:	Wed Nov 23 14:15:10 CST 2005
Description:	
Owner:	ccRoot
Close	

Java.Applet Window

Figure 244 Task Details

Note: If a task is changed or updated, its prior history no longer applies and the “Last Execution Date” will be blank.

Notification Manager

Use Notification Manager to configure an external SMTP server so notifications can be sent from CC-SG. Notifications are used to email reports that have been scheduled, email reports if users are locked out, email status of failed or successful scheduled tasks—please see section **Task Manager** earlier in this chapter for additional information. After configuring the SMTP server, you can elect to send a test email to the designated recipient and notify the recipient of the result of the test.

To configure an external SMTP server:

1. On the **Setup** menu, click **Notification Manager**.

Figure 245 Notification Manager

2. Ensure **Enable SMTP Notification** is selected and type the **SMTP host**. For hostname rules, see **Terminology/Acronyms** in **Chapter 1: Introduction**.
3. Type a valid **SMTP port**.
4. Type a valid **Account name** for logging onto the SMTP server.
5. Type and confirm the **Password** for the SMTP account.
6. Type a valid **From** email address that will identify the message is from CC-SG.
7. Specify a number for the number of **Retries** in the case the email fails to be sent.
8. Type a number, in minutes, for the **Retry Interval** that will be used before the email is sent again in the event the email fails.
9. Check **Use SSL** if you want the email to be sent securely over Netscape's Secure Sockets Layer (SSL).
10. Click **Test Configuration** to send an email to the SMTP account specified.
11. Click **Update Configuration** to save your changes.

SSH Access to CC-SG

Use Secure Shell (SSH) clients, such as Putty or OpenSSH Client, to access a command line interface to SSH (v2) server on CC-SG. Only a subset of CC-SG commands is provided via SSH to administer devices and CC-SG itself.

The SSH client user is authenticated by the CC-SG in which existing authentication and authorization policies are applied to the SSH client. The commands available to the SSH client are determined by the permissions for the user group(s) to which the SSH client user belongs.

Administrators who use SSH to access CC-SG cannot logout a **ccroot** SSH user, but are able to log out all other SSH client users, including Administrators.

1. Launch a SSH client, such as Putty.
2. Enter the IP address of the CC-SG and specify **22** for the port. You can permanently configure the port for SSH access in Security Manager—see **Configure Security** earlier in this chapter for additional information.

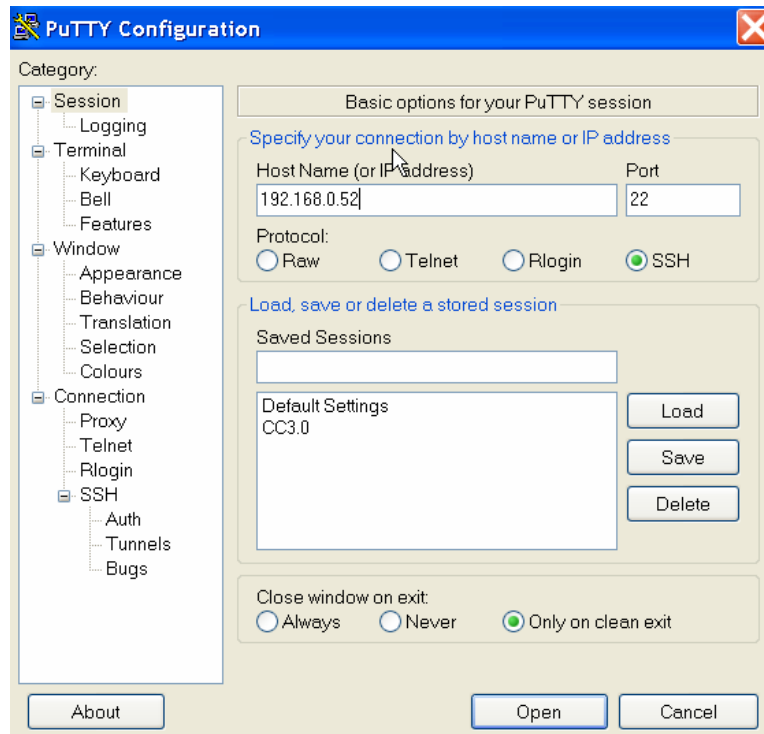


Figure 246 SSH Client

3. Click **Open**. A window opens, prompting you for the CC-SG login and password. Type CC-SG login and password (default is **ccroot/raritan0**).



Figure 247 Login to CC-SG via SSH

4. A shell prompt appears. Type **ls** to display all commands available from SSH.

```

[CommandCenter ccRoot]$ ls
activeports      activeusers      backupdevice
clear            connect          copydevice
disconnect       entermaint       exit
exitmaint        grep             help
listbackups     listdevices      listfirmwares
listports        logoff           ls
more            pingdevice       portcatalog
restartcc        restartdevice    restoredevice
shutdowncc       ssh              su
upgradedevice

[CommandCenter ccRoot]$

```

Figure 248 CC-SG Commands via SSH

5. Typing **help** or **?** provides the syntax and description of all available commands.

```

[CommandCenter ccRoot]$ help
CommandCenter Secure Gateway SSH, version 3.0.0.2.7
Type 'command -h' to find out more about the function 'command'.

List of commands:

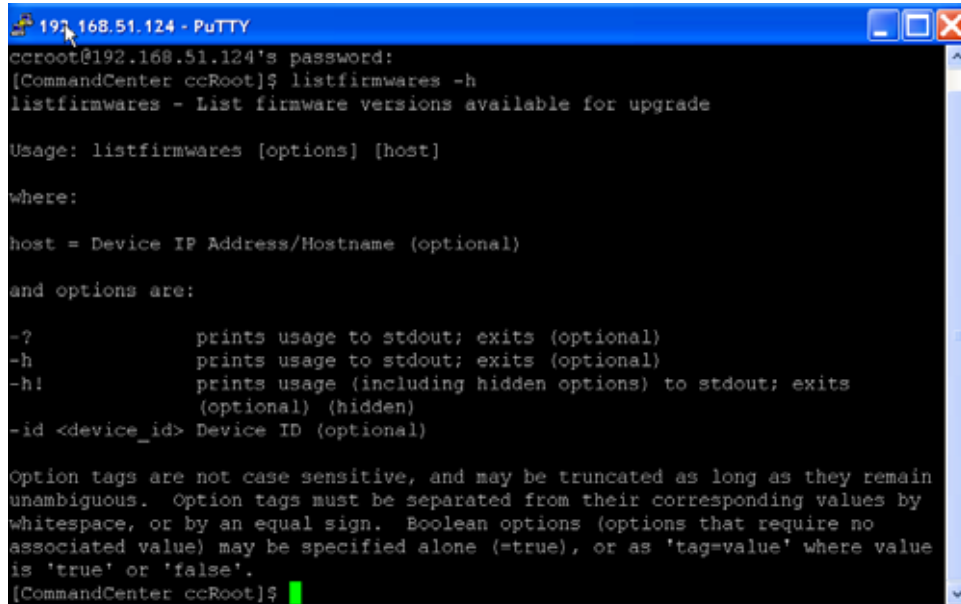
Usage                                     Descript
ion

activeports                             List act
ive ports
activeusers                             List act
ive users
backupdevice [-id <device_id>] [-host <host>] backup_name [description] Backup d

```

Figure 249 SSH Help

6. Typing the command with the **-h** switch displays help for that command, such as **listfirmwares -h**.



```
192.168.51.124 - PuTTY
ccroot@192.168.51.124's password:
[CommandCenter ccRoot]$ listfirmwares -h
listfirmwares - List firmware versions available for upgrade

Usage: listfirmwares [options] [host]

where:

host = Device IP Address/Hostname (optional)

and options are:

-?          prints usage to stdout; exits (optional)
-h          prints usage to stdout; exits (optional)
-h!         prints usage (including hidden options) to stdout; exits
            (optional) (hidden)
-id <device_id> Device ID (optional)

Option tags are not case sensitive, and may be truncated as long as they remain
unambiguous. Option tags must be separated from their corresponding values by
whitespace, or by an equal sign. Boolean options (options that require no
associated value) may be specified alone (=true), or as 'tag=value' where value
is 'true' or 'false'.
[CommandCenter ccRoot]$
```

Figure 250 SSH listfirmwares Help

Command Tips

The following describes several nuances of the SSH commands:

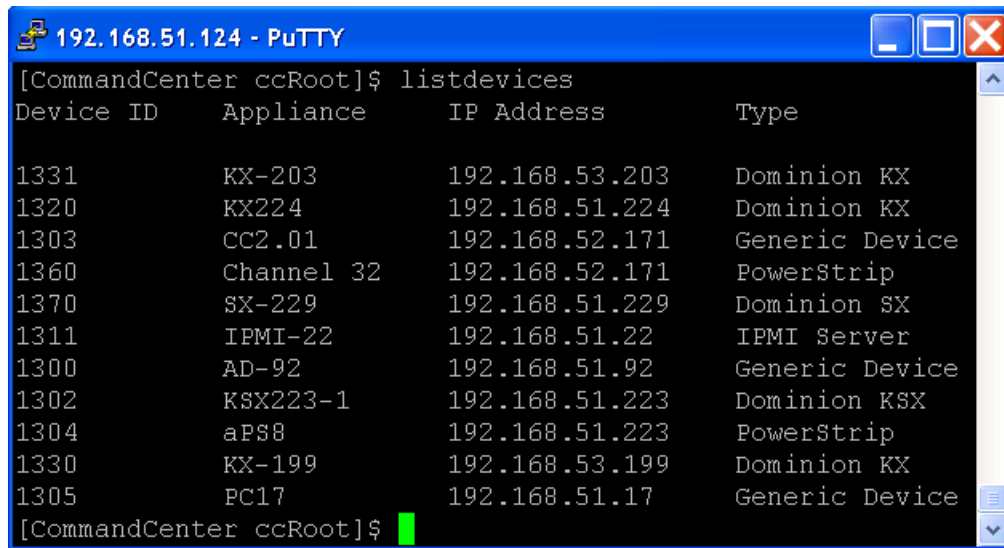
- For commands that pass an IP address, such as **upgradedevice**, you can substitute the hostname for an IP address. For hostname rules, see Terminology/Acronyms in **Chapter 1: Introduction**.
- The **copydevice** and **restartdevice** commands apply only to some Raritan devices, for example, Dominion SX. IPMI servers, generic devices are not supported by these commands.

Create a SSH Connection to an SX Device

You can create an SSH connection to an SX device to perform administrative operations on the device. Once connected, the administrative commands supported by the SX device are available.

Note: Before you can connect, ensure that the SX device has been added to the CC-SG.

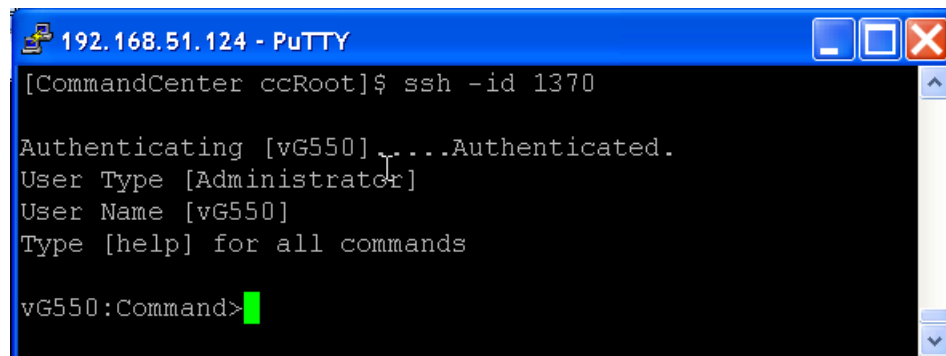
1. Type **listdevices** to ensure the SX has been added to CC-SG.



```
[CommandCenter ccRoot]$ listdevices
Device ID      Appliance      IP Address      Type
-----
1331           KX-203         192.168.53.203  Dominion KX
1320           KX224         192.168.51.224  Dominion KX
1303           CC2.01        192.168.52.171  Generic Device
1360           Channel 32    192.168.52.171  PowerStrip
1370           SX-229        192.168.51.229  Dominion SX
1311           IPMI-22       192.168.51.22   IPMI Server
1300           AD-92         192.168.51.92   Generic Device
1302           KSX223-1     192.168.51.223  Dominion KSX
1304           aPS8         192.168.51.223  PowerStrip
1330           KX-199       192.168.53.199  Dominion KX
1305           PC17         192.168.51.17   Generic Device
[CommandCenter ccRoot]$
```

Figure 251 Listing Devices on CC-SG

2. Connect to the SX device by typing **ssh -id <device id>** or **ssh <IP Address/Host>**. For example, using above screen , you can connect to SX-229 by typing **ssh -id 1370**.



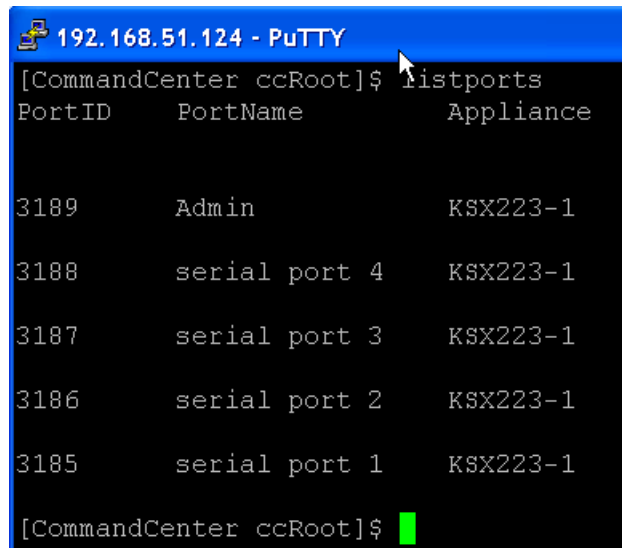
```
[CommandCenter ccRoot]$ ssh -id 1370
Authenticating [vG550]...Authenticated.
User Type [Administrator]
User Name [vG550]
Type [help] for all commands
vG550:Command>
```

Figure 252 Access SX Device via SSH

Connect to a Serial Port

Connect to a serial port to access a target server. You can access serial ports on a SX, KSX, or IP-Reach device. The SSH connection to the serial ports are in proxy mode.

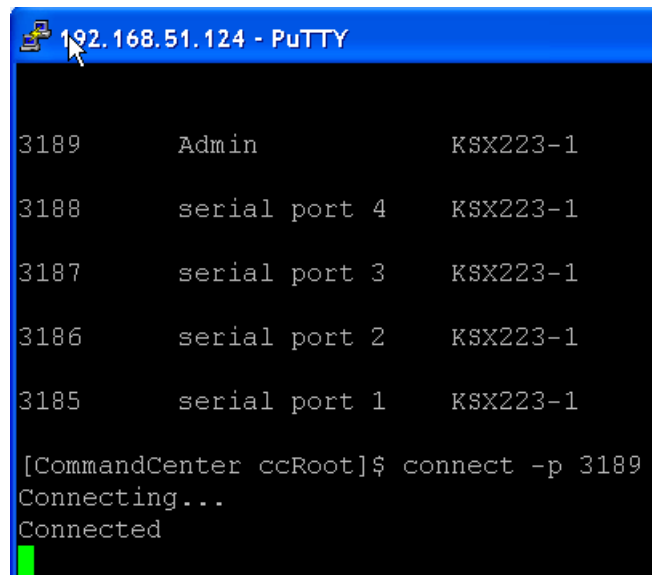
1. Type **listports** to view the port ids.



```
192.168.51.124 - PuTTY
[CommandCenter ccRoot]$ listports
PortID      PortName      Appliance
-----
3189        Admin         KSX223-1
3188        serial port 4 KSX223-1
3187        serial port 3 KSX223-1
3186        serial port 2 KSX223-1
3185        serial port 1 KSX223-1
[CommandCenter ccRoot]$
```

Figure 253 Listing Ports on CC-SG

2. Type **connect -p <port id>** to connect to the target server associated with the port.



```
192.168.51.124 - PuTTY
3189        Admin         KSX223-1
3188        serial port 4 KSX223-1
3187        serial port 3 KSX223-1
3186        serial port 2 KSX223-1
3185        serial port 1 KSX223-1
[CommandCenter ccRoot]$ connect -p 3189
Connecting...
Connected
[CommandCenter ccRoot]$
```

Figure 254 Connecting to a Serial Port

- Once connected to the port, type the default Escape keys of '~' followed by a dot '.'. An intermediate prompt, typically named after port name, is displayed, for example **testport>**. At this intermediate prompt, you can enter specific commands or aliases as described below:

COMMAND	ALIAS	DESCRIPTION
quit	q	Terminates Port Connection and returns to SSH prompt.
get_write	gw	Gets Write Access. Allows SSH user to execute commands at target server while browser user can only observe proceedings in the port.
get_history	gh	Gets History. Displays the last few commands and results at target server.
send_break	sb	Sends Break. Breaks the loop in target server initiated by browser user.
help	?,h	Prints help screen.

From the CC-SG GUI, you can view an Active Report that displays connections initiated by SSH clients. To view ports that are busy and have connections initiated by SSH clients, you can run a Query Port. Please see Chapter 10: Generating Reports for additional information.

Exit a Session

To exit the entire SSH connection to CC-SG, type **exit**.

Diagnostic Console

The Diagnostic Console is a standard, non-graphical interface that provides local access to CC-SG. It can be accessed from a serial or KVM port, or from Secure Shell (SSH) clients, such as Putty or OpenSSH Client.

Two logins are provided—one is **status** and the other is **admin**. Default password for **admin** is **raritan**. All login usernames and passwords are case-sensitive. Logging in as **status** displays current system information to ascertain the health of CC-SG. The **admin** account allows you to set initial parameters, view log files, and perform some limited diagnostics such as changing the IP address of the CC-SG or restarting CC-SG.

***Note:** If accessing Diagnostic Console via SSH, the Status Console and the Administrator Console inherits the appearance settings that are configured in your SSH client and keyboard bindings.*

Accessing Diagnostic Console via SSH

1. Launch a SSH client, such as Putty.
2. Enter the IP address, or IP hostname if CC-SG has been registered with a DNS server, of the CC-SG and specify **23** for the port.

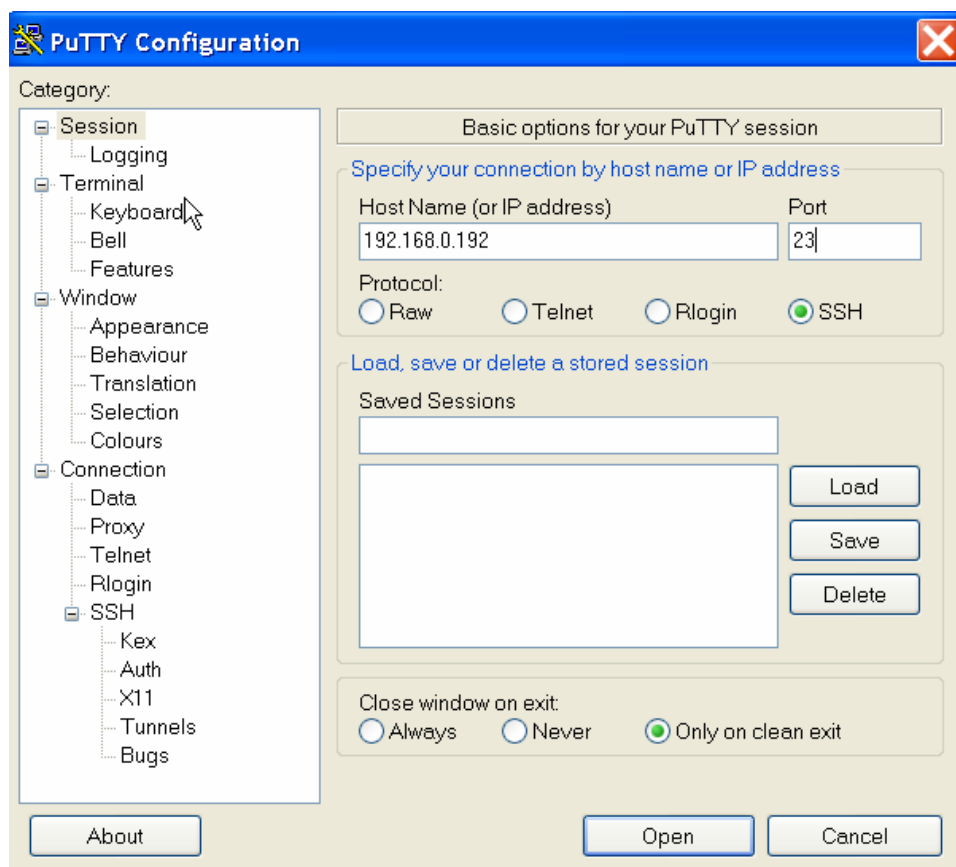


Figure 255 SSH Client

3. Click **Open**. A window opens, prompting you for a login.

Accessing Status Console

Entering a password to access the Status Console is not required, but can be enforced if desired.

1. After **login as:**, type **status**.



Figure 256 Login to Status Console

The read-only status console is displayed. This screen dynamically displays information to help you determine the health of your system and if CC-SG and its sub-components are working. The time in the upper-right corner of the screen is the last time on the CC-SG the data was polled.

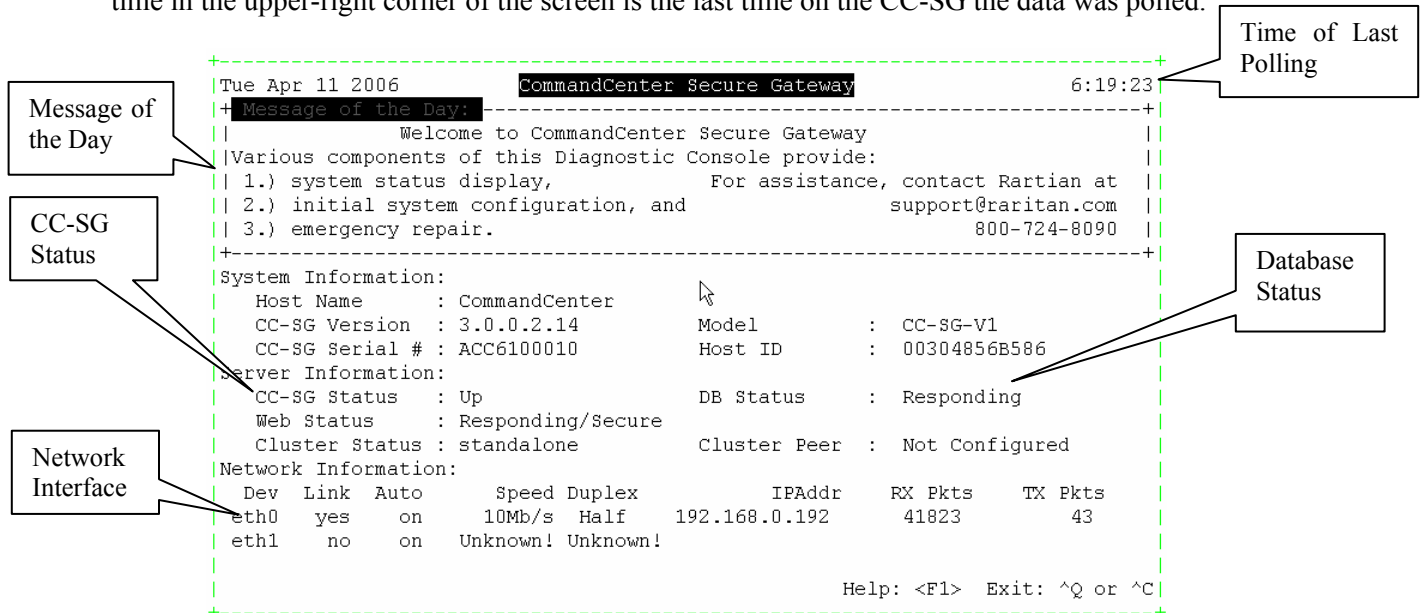


Figure 257 Status Console

Important information to hone in on includes the **Up** status for CC-SG and other sub-components, such as Database. If it is **Down**, it may be in the process of rebooting. Or, if Down is continual, you may want to call Raritan Technical Support or try restarting CC-SG with the admin account in Diagnostic Console. Other information displayed includes: CC-SG software version, cluster configuration, web status, etc.

2. Exit the window by pressing **Ctrl-Q** or **Ctrl-C**.

Accessing Administrator Console

At the time of logging into Administrator Console, all information displayed is “static”. If configuration changes occur through the CC-SG GUI or the Diagnostic Console, you need to re-login to Administrator Console after the changes have taken effect to view the changes in Administrator Console.

1. After **login as:**, type **admin**.

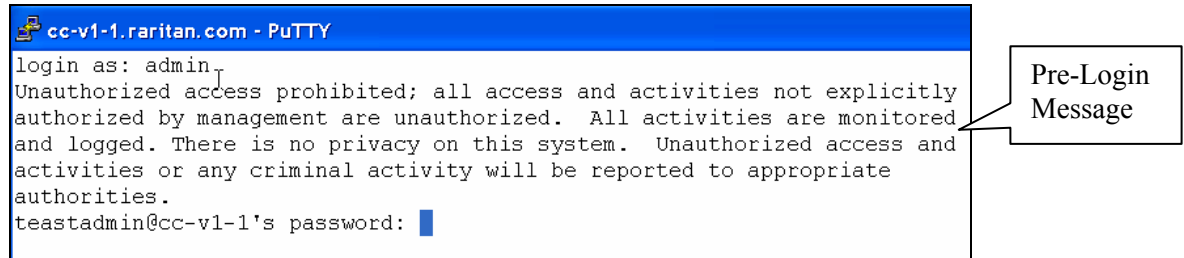


Figure 258 Login to Administrator Console

2. Type the CC-SG password (**raritan** is the default). Re-enter this password and when prompted, type a new password. See section **Changing Passwords (Admin)** later in this chapter for details on setting password strength.

The Administrator Console is then displayed. In this window, you can perform initial system network interface configuration, edit Message of the Day in the Status window, and view log files.

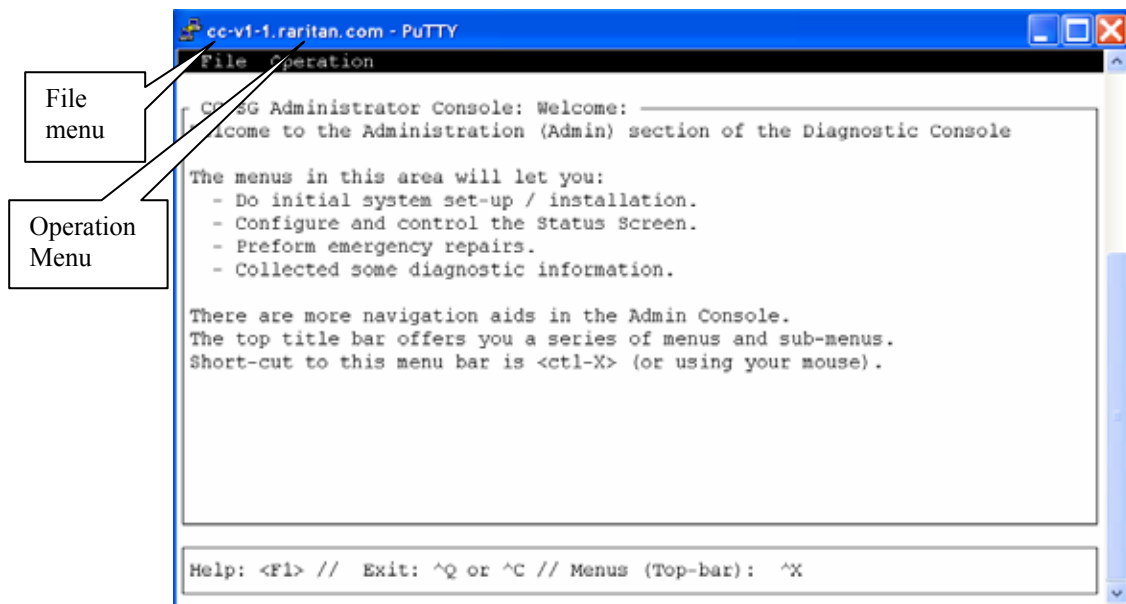


Figure 259 Administrator Console

Navigating Administrator Console

PRESS..	To...
CTRL+C or CTRL+Q	To exit Diagnostic Console.
CTRL+L	Refresh screen and update information.
TAB	Move to next available option.
SPACE	Select current option.
Arrow Keys	Allows you to move to various options.
Mouse	Allows you to point and select an option.

Editing Pre-Login Message/MOTD (Status Console)

The Pre-Login message appears in the Administrator Console after entering any login username and before entering the password. The Message of the Day (MOTD) appears at the top of the Status Console.

- To edit the Pre-Login or MOTD message, click **Operation**, **Status Console**, then **Edit Pre-Login Message** or **Edit MOTD**.

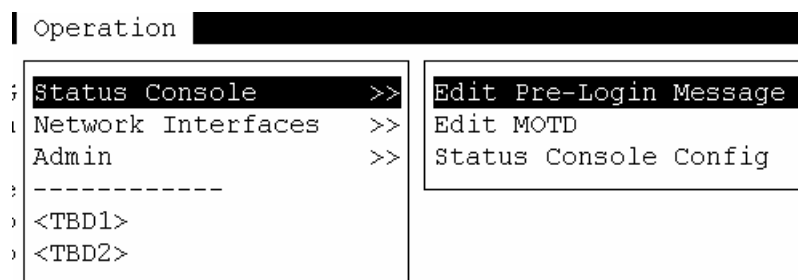


Figure 260 Selecting to Edit Pre-Login Message

- Using the **Delete** and **Backspace** keys, type a new message in the box provided. For Message of the Day, the height is fixed and up to 76 characters can be entered.

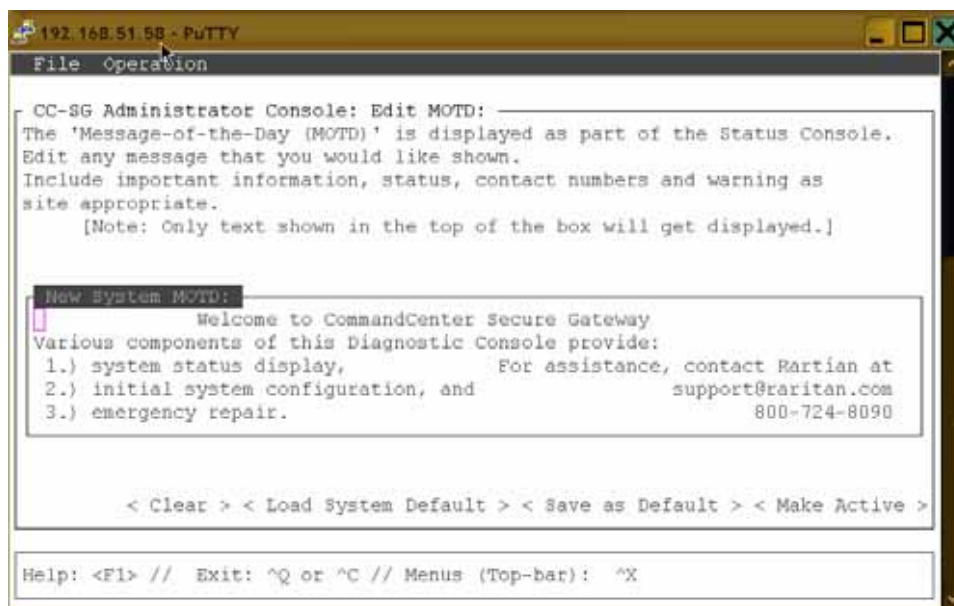


Figure 261 Editing MOTD for Status Console

- Click **Save as Default** at the bottom of the screen or press the **TAB** key and press **Enter** once Save as Default is highlighted. Press **^Q** or **^C** to exit.

The Pre-Login and Message of the Day have three separate buffers or areas:

- Admin Console Screen – starts with a copy of the Active Message and can be edited by this user / session.
- A system buffer that is held across system resets.
- The Active Message buffer (as seen by users when they interact with the system).

BUTTON	DESCRIPTION
Clear	Removes all text in the currently displayed Admin Console screen. Has no effect on the value used by the system.
Load System Default	Replaces the Admin Console Screen with the contents of the System Buffer.
Save as Default	Puts the current Admin Console Screen into System Buffer. Has no effect on the Active Message display.
Make Active	Replaces the current Active Message with the contents of the Admin Console screen. All new users will see the new message.

Editing Status Console Configuration (Status Console)

The Diagnostic Console can be accessed from a serial or KVM port, or from Secure Shell (SSH) clients. For each port type, you can configure whether or not status or admin logins are allowed and if field support can also access Diagnostic Console from the port. For SSH, you can also configure the port number to be used.

- To edit status console configuration, click **Operation**, **Status Console**, then **Status Console Config**.

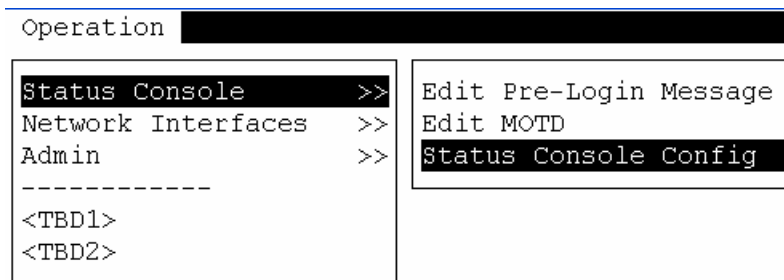


Figure 262 Selecting to Edit Status Console Config

- Click or use the **TAB** key, **↓↑** keys, and **Enter** keys to determine what you want displayed in status console. There are three Diagnostic Console Access mechanisms:

- Serial Port (COM1)
- KVM Console
- SSH (IP network)

The Diagnostic Console offers three services:

- Status Display
- Admin Console
- Raritan Field Support

This screen allows the selection of which services are available via the various access mechanisms.

Important: Be careful not to completely lock-out all Admin or Field Support access.

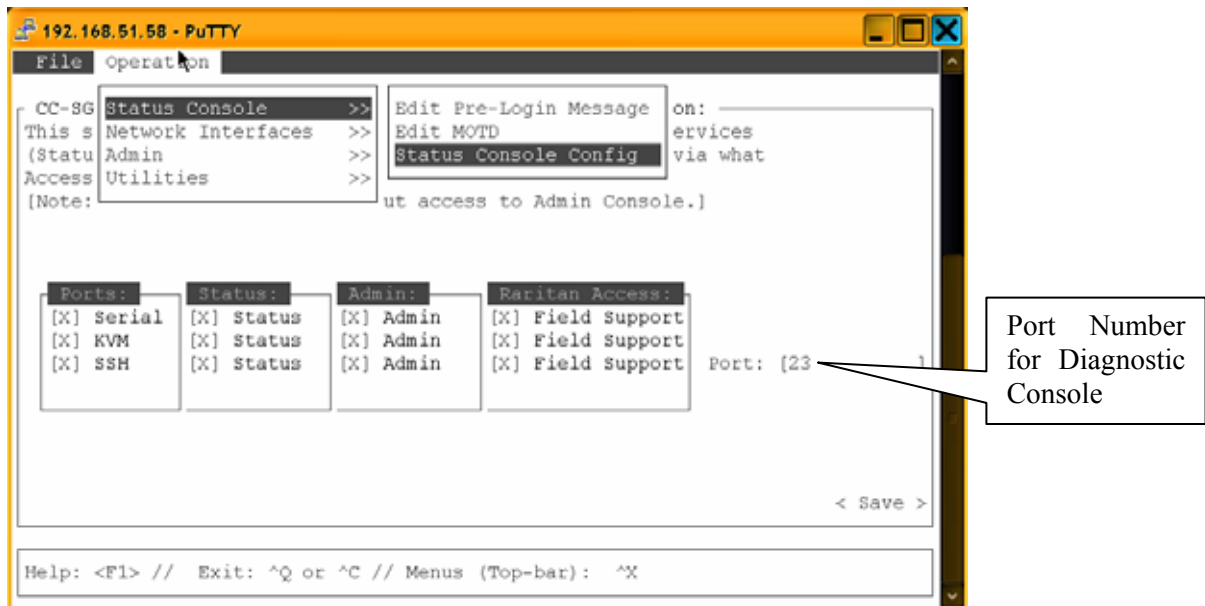


Figure 263 Edit Status Console Config

3. Click **Save** at the bottom of the screen or press the **TAB** key and press **Enter** once Save is highlighted. Press **^Q** or **^C** to exit.

Editing Network Interfaces Configuration (Network Interfaces)

In Network Interface Configuration, you can perform initial setup tasks such as setting the hostname and IP address of the CC-SG. Click with the mouse or use the **TAB**, **↓↑** keys to navigate and press the **Enter** key to select a value.

1. To edit network interface information, click **Operation**, **Network Interfaces**, then **Network Interface Config**.

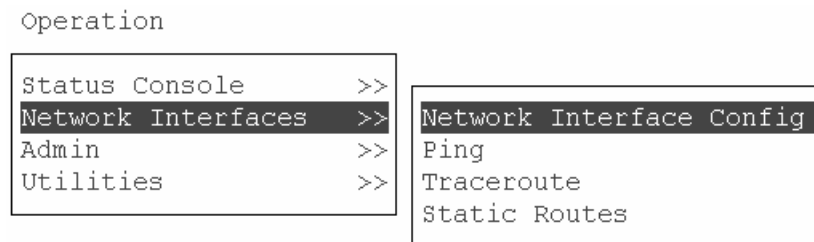


Figure 264 Selecting Network Interface Configuration

- If this is the first time accessing CC-SG and the network interfaces have not been configured, it is strongly recommended to use CC-SG GUI to configure them instead of configuring them here. If the network interfaces have already been configured, you will see a Warning message, stating that you should use the CC-SG GUI to configure the interfaces. If you want to continue, click **YES**.

File Operation

CC-SG Administrator Console: Network Interface Configuration:

Hostname: [CommandCenter]	
Domain Suffix: [ignored]	
Primary DNS: []	Secondary DNS: []
Mode: <O> Primary/Backup < > Active/Active	
Configuration: < > DHCP <O> STATIC	Configuration: < > DHCP <O> STATIC
IP Address: [192.168.0.192]	IP Address: []
Netmask: [255.255.255.0]	Netmask: []
Gateway: []	Gateway: []
Adapter Speed: <O> AUTO	Adapter Speed: <O> AUTO
Adapter Duplex: <O> HALF	Adapter Duplex: <O> HALF
< Save >	

Help: <F1> // Exit: ^Q or ^C // Menus (Top-bar): ^X

Figure 265 Editing Network Interfaces

- Type your hostname in the **Host Name** field. Once **Save** is selected (and Admin Console re-entered or on the CC-SG GUI), this field will be updated to reflect the Fully-Qualified Domain Name (FQDN) if known. For hostname rules, see **Terminology/Acronyms** in **Chapter 1: Introduction**.
- Click appropriate option button for either **Primary/Backup Mode** or **Active/Active Mode**. See section **Network Configuration** earlier in this chapter for details.
- Click either **DHCP** or **Static** from the list.
 - If you choose DHCP and your DHCP server has been configured correctly, the DNS information, the domain suffix, IP address, default gateway and subnet mask will be automatically populated once **Save** is selected and you exit and re-enter Admin Console.
 - If you choose **Static**, type an **IP address**, **subnet mask**, **default gateway**, **Primary DNS** and **Secondary DNS** information, and string for your domain setup in **domain suffix**.
- Click **Adapter Speed** and use the ↓↑ keys to select a line speed from the list.
- If you did not select **AUTO** for **Adapter Speed**, click **Adapter Duplex** and use the ↓↑ keys to select a duplex mode from the list, if applicable.
- Repeat steps 6 through 8 for the second network interface if you selected **Active/Active Mode**.
- Click **save** to save your changes. CC-SG will be restarted and will log off all CC-SG GUI users and terminate their session.

Ping an IP Address (Network Interfaces)

Use ping to check that the connection between your computer and a particular IP address (domain) is working correctly.

1. To ping an IP address or hostname, click **Operation**, **Network Interfaces**, then **Ping**.

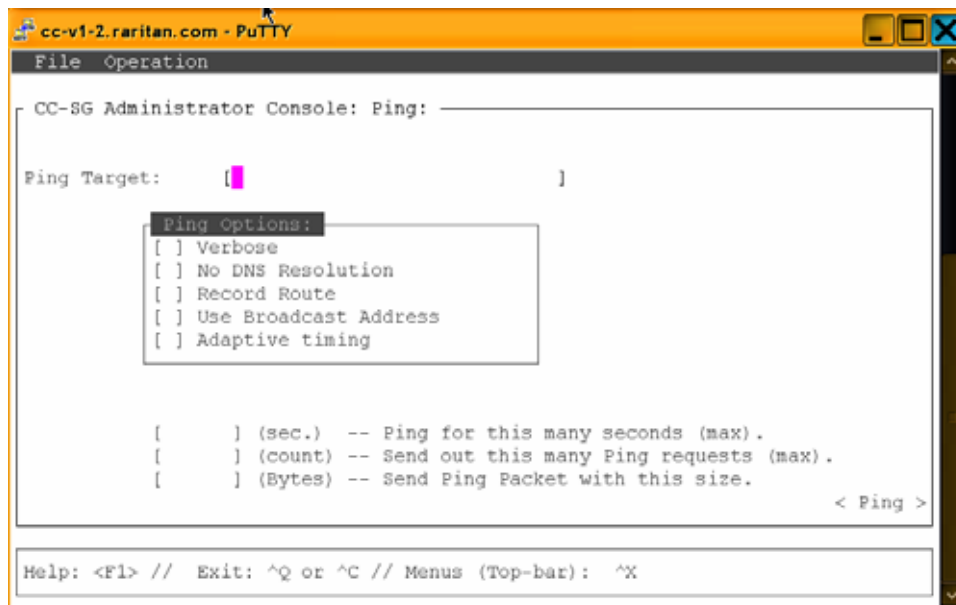


Figure 266 Pinging a Target

2. Enter the IP address or hostname of the target you wish to check in the **Ping Target** field.
3. Optionally, select:

OPTION	DESCRIPTION
Verbose	Verbose output, which lists other received ICMP packets in addition to ECHO_RESPONSE packets.
No DNS Resolution	Does not resolve addresses to host names.
Record Route	Records route. Sets the IP record route option, which will store the route of the packet inside the IP header.
Use Broadcast Address	Allows pinging a broadcast message.
Adaptive Timing	Adaptive ping. Interpacket interval adapts to round-trip time, so that effectively not more than one unanswered probes present in the network. Minimal interval is 200 msec.

4. Optionally, type values for how many seconds the ping command will execute, how many ping requests are sent, and the size for the ping packets (default is 56, which translates into 64 ICMP data bytes when combined with 8 bytes of ICMP header data). If left blank, defaults will be used.
5. Click **Ping** in the bottom right-hand corner of the window. If the results show a series of replies, the connection is working. The time shows you how fast the connection is. If you see a "timed out" error instead of a reply, there is a breakdown somewhere between your computer and the domain. In this case, the next step is to perform a traceroute – see the next section.
6. Press **CTRL+C** to terminate the ping session.

Note: Pressing **CTRL+Q** displays a statistics summary for the session so far and continues to ping the destination.

Using Traceroute (Network Interfaces)

Traceroute is often used for network troubleshooting. By showing a list of routers traversed, it allows you to identify the path taken from your computer to reach a particular destination on the network. It will list all the routers it passes through until it reaches its destination, or fails to and is discarded. In addition to this, it will tell you how long each 'hop' from router to router takes. This can help identify routing problems or firewalls that may be blocking access to a site.

1. To perform a traceroute on an IP address or hostname, click **Operation, Network Interfaces**, then **Traceroute**.

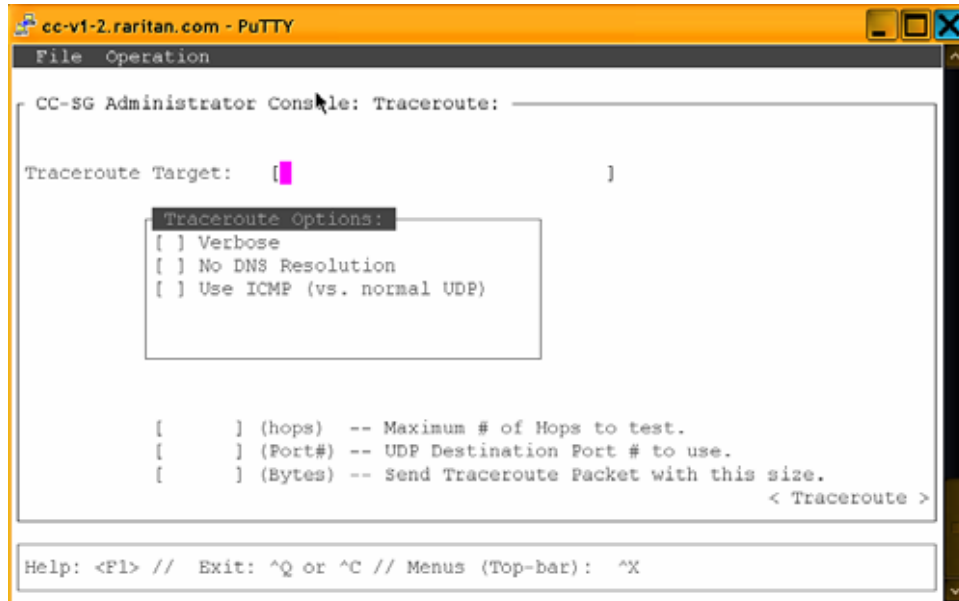


Figure 267 Performing Traceroute on a Target

2. Enter the IP address or hostname of the target you wish to check in the **Traceroute Target** field.
3. Optionally, select:

OPTION	DESCRIPTION
Verbose	Verbose output, which lists received ICMP packets other than TIME_EXCEEDED and UNREACHABLEs.
No DNS Resolution	Does not resolve addresses to host names.
Use ICMP (vs. normal UDP)	Use ICMP ECHO instead of UDP datagrams.

4. Optionally, type values for how many hops the traceroute command will use in outgoing probe packets (default is 30), the UDP destination port to use in probes (default is 33434), and the size for the traceroute packets. If left blank, defaults will be used.
5. Click **Traceroute** in the bottom right-hand corner of the window.
6. Press **CTRL+C** or **CTRL+Q** to terminate the traceroute session. A **Return?** prompt appears; press **ENTER** to return to the Traceroute menu. The **Return?** prompt also appears when Traceroute terminates due to “destination reached” or “hop count exceeded” events occur.

Editing Static Routes (Network Interfaces)

In Static Routes, you can view the current IP routing table and modify, add, or delete routes. Careful use and placement of static routes may actually improve the performance of your network, allowing you to conserve bandwidth for important business applications and may be useful for

Active/Active network settings where each interface is attached to a separate IP domain—see section **Network Configuration** in **Chapter 12: Advanced Administration** for additional information. Click with the mouse or use the **TAB**, **↓**/**↑** keys to navigate and press the **Enter** key to select a value.

1. To view or change static routes, click **Operation**, **Network Interfaces**, then **Static Routes**.

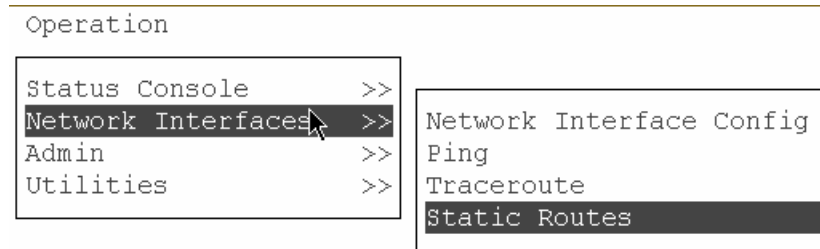


Figure 268 Selecting Static Routes

2. The current IP routing table is displayed. You can add a host or network route, or delete a route.

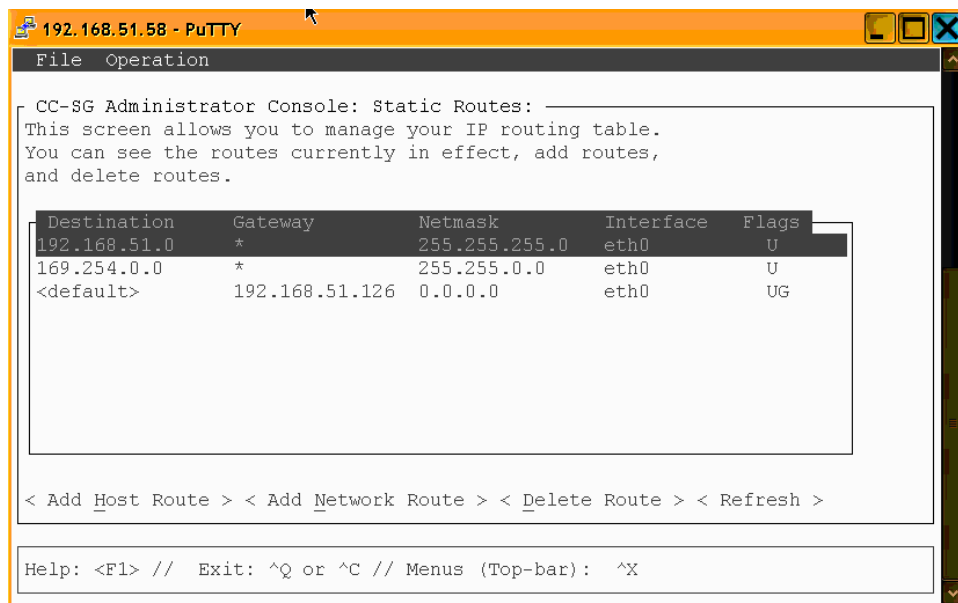


Figure 269 Editing Static Routes

Viewing Log Files (Admin)

You can view one or more log files simultaneously via LogViewer, which allows browsing through several files at once, to examine system activity.

1. To view log files, click **Operation**, **Admin**, then **System Logfile Viewer**.

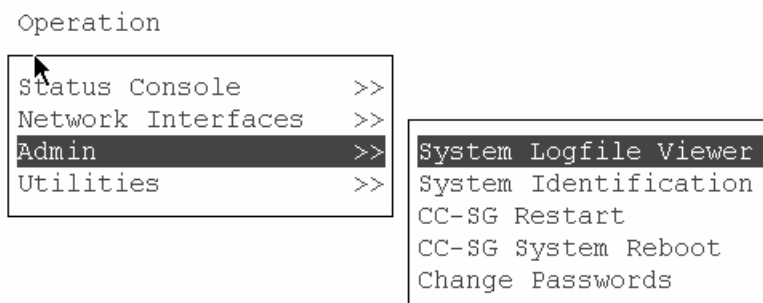


Figure 270 Viewing Log Files

2. Click with the mouse or use the $\downarrow\uparrow$ keys to navigate and press the **Enter** key to select a log file (marked with an **X**). More than one log file can be viewed at a time. (Some log files are not available; a warning dialog will appear and the item will be de-selected for you.)

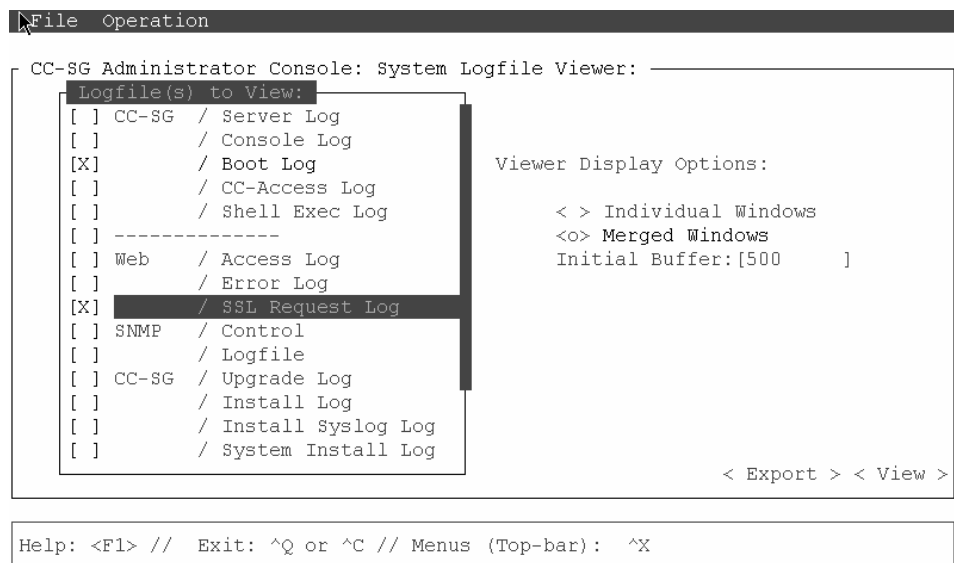


Figure 271 Selecting Log Files to View

OPTION	DESCRIPTION
Individual Windows	Display the selected logs in separate windows.
Merged Windows	Merge the selected logs into one window.
Initial Buffer	Sets initial buffer or history size. 500 is default. This system is configured to buffer all the new information that comes along.
Export	Available to Field Support only in this release.
View	View the selected log(s).

3. When **View** is selected with Merged Windows, the LogViewer displays:

```

cc-v1-1.raritan.com - PuTTY
service,service=Logging
16:02:57,429 DEBUG [Log4jService] Creating jboss.system:type=Log4jService,service=Logging
16:02:57,430 INFO [Log4jService$URLWatchTimerTask] Configuring from URL: resource:log4j.xml
00] /sg/logs/jboss/boot.log 55062 - Wed Dec 14 16:02:57 2005
'dCenter' does NOT match server name!
[Mon Jan 09 10:51:43 2006] [warn] RSA server certificate CommonName (CN) 'CommandCenter' does NOT match server name!
[Mon Jan 09 10:51:43 2006] [notice] Apache configured -- resuming normal operations
01] /opt/apache/logs/error log 51926 - Mon Jan 9 10:51:43 2006
[Unloading class sun.reflect.GeneratedSerializationConstructorAccessor10038]
[Unloading class sun.reflect.GeneratedSerializationConstructorAccessor10032]
52902K->48895K(324096K), 0.4741690 secs]
[Full GC 52822K->48963K(324096K), 0.4426160 secs]
[Full GC 52625K->49025K(324096K), 0.4462180 secs]
02] /sg/logs/jboss/console.log 2632839 - Mon Jan 9 16:14:01 2006
-----
Process ended (Wed, 14 Dec 2005 15:59:46 -0500).
-----
03] /sg/logs/ShellCommandExecutor.log 2993 - Wed Dec 14 15:59:46 2005

```

Figure 272 Selecting Log Files to View

4. While viewing log files, type **CTRL+C** to return to the previous screen.
5. If desired, you can change colors in a log file to highlight what is important. Type **c** to change colors of a log file and select a log from the list if you have chosen to view several. Once color choices are displayed, type **q** to exit the window.

```

Toggle colors: se
00 /sg/logs/jbos
01 /opt/apache/l
02 /sg/logs/jbos
03 /sg/logs/Shel
Press ^G to abort

```

Figure 273 Changing Colors in Log Files

6. Type **i** for info to display system information.

Note: System load is static as of the start of this Admin Console session – use the **TOP** utility to dynamically monitor system resources.

```

==* MultiTail 3.8.10 *==

Written by folkert@vanheusden.com
Website: http://www.vanheusden.com/multitail/

Current load of system: 0.21 0.10 0.08

Running on:
CC-V1-2.raritan.com/Linux
2.6.9-22.0.1.EL #1 Thu Oct 27 12:26:11 CDT 2005
i686
Terminal size: 80x24

Press any key to exit this screen

```

Figure 274 Displaying Information

7. If desired, you can filter the log file with a regular expression. Type **e** to add or edit a regular expression and select a log from the list if you have chosen to view several.

```
Select window (re
e00 /sg/logs/jbos
01 /opt/apache/l
02 /sg/logs/jbos
03 /sg/logs/Shel
Press ^G to abort
```

Figure 275 Adding Expressions in Log Files

8. Type **a** to add a regular expression. For example, if you want to display information on the **pam** process in **/var/log/messages** log file, enter **pam** and select **match**.

```
Edit reg.exp.
/sg/logs/jboss/boot.log
add, edit, delete, quit

Edit regular expression:
>pam

Usage of regexp? (match, v do not match
Color, Bell, bell + colorize, execute)
```

Figure 276 Specifying a Regular Expression for a Log File

9. Select **F1** to get help on all LogViewer options. Pressing **CTL+C** and **CTL+Q** (as well as a plain **q**) terminates this LogViewer session.

```

Use cursor UP/DOWN to scroll, ctrl+g to exit
One can press the following keys:
q      quit the program
F1     this help
a      add a new window or add another file/
      program to an existing window
d      delete a window (or a file/program from a
      window)
s      swap the location of 2 windows
e      enter/edit regular expressions
c      set/change colors (only works if your
      terminal supports colors)
b      scrollbar in the buffer of a window
v      toggle vertical split
0...9  set a mark in a window so that you can
      easily see what has changed since the last

```

Figure 277 Getting Help (F1)

Restarting CC-SG (Admin)

You can restart CC-SG, which will log off all current CC-SG users and terminate their sessions to remote target servers.

Important: It is is **HIGHLY** recommended to restart CC-SG in the CC-SG GUI instead, unless it is absolutely necessary to restart it here. See section **Restart CC-SG** in Chapter 11: System Maintenance for additional information. Restarting CC-SG in Diagnostic Console will **NOT** notify CC-SG GUI users that it is being restarted.

1. To restart CC-SG, click **Operation**, **Admin**, then **CC-SG Restart**.

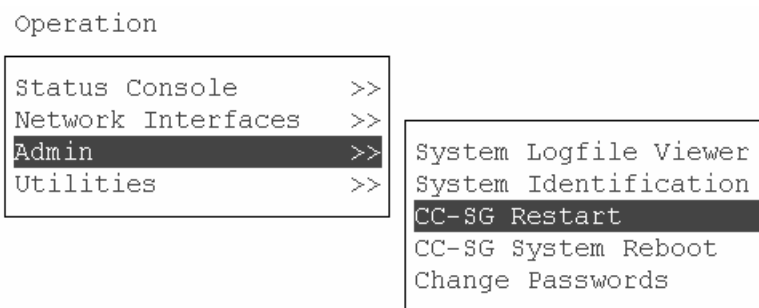


Figure 278 Selecting CC-SG Restart in Diagnostic Console

2. Either click **Restart CC-SG Application** or press **ENTER**.

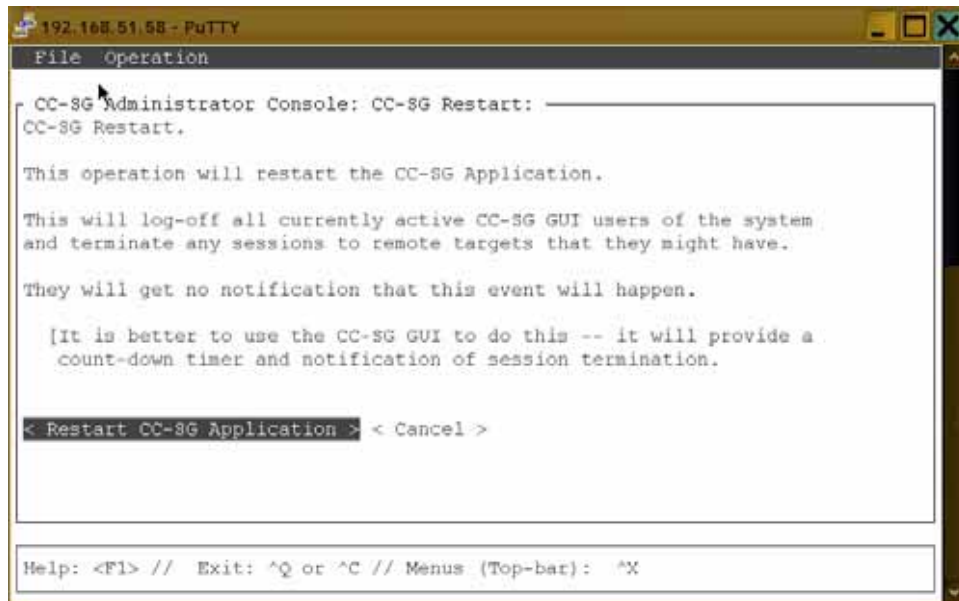


Figure 279 Restarting CC-SG in Diagnostic Console

Rebooting CC-SG (Admin)

This option will reboot the entire CC-SG, which simulates a power cycle. Users will NOT receive a notification at all. CC-SG, SSH, and Diagnostic Console users (including this session) will be logged off. Any connections to remote target servers will also be terminated.

1. To reboot CC-SG, click **Operation**, **Admin**, then **CC-SG System Reboot**.

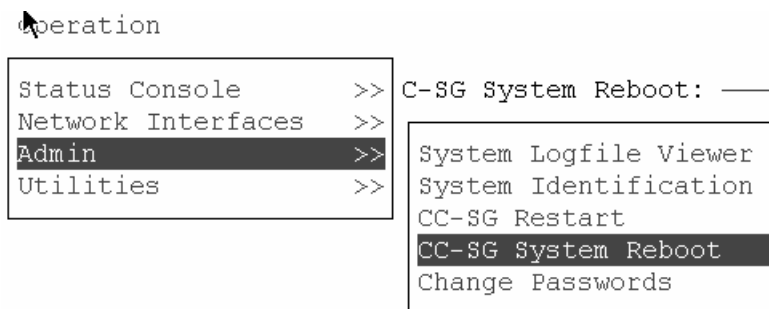


Figure 280 Selecting CC-SG System Reboot in Diagnostic Console

2. Either click **REBOOT System** or press **ENTER** to reboot CC-SG. A screen to confirm this action appears and needs to be acknowledged before this operation will commence.

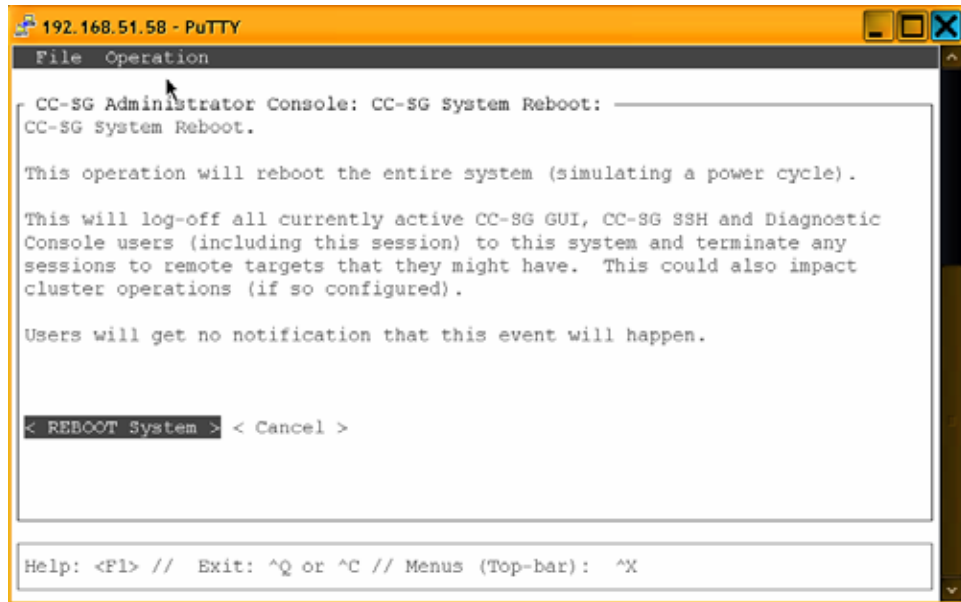


Figure 281 Rebooting CC-SG in Diagnostic Console

Changing Passwords (Admin)

This option provides the ability to configure the strength of passwords (status and admin) and allows you to configure password attributes, such as, the setting maximum number of days that must lapse before you need to change the password, which should be done via the Account Configuration menu.

Password Configuration

The settings configured here affect only the **admin** and **status** (if enabled) passwords upon the next password change.

To change password settings, click **Operation**, **Admin**, **Change Passwords**, then **Password Configuration**.

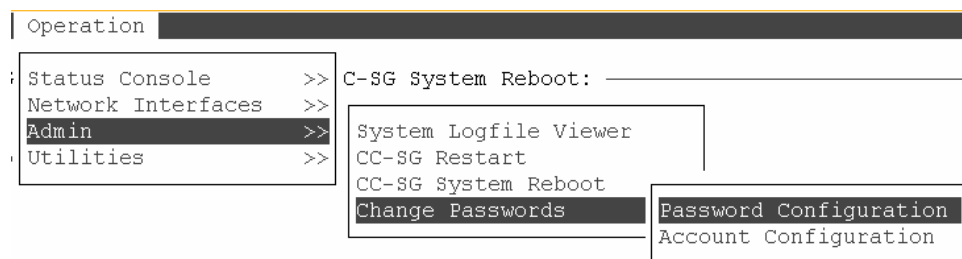


Figure 282 Password Configuration

In **Password Configuration**, enter the number of passwords that will be remembered. This is the password history, which discourages password reuse and ensures that the new password has not been used within the specified number of previous password changes. Default is 5. With a setting of 5, the new password could not have been used within the last 5 password changes.

```

File  Operation

CC-SG Administrator Console: Password Settings:
Use this screen to update how all subsequent Diagnostic Console (only!)
password operations will work. You can set the type of passwords (regular,
strong or random) that the system will let the user use on any subsequent
password change operation. Also, the number of passwords henceforth that
the system will remember and not let the user duplicate or reuse.

Password Configuration:

Password History Depth: [ 5 ]

Password Type & Parameters:
<O> Regular
< > Random  Size:[20 ] Retries:[10 ]
< > Strong  Retries:[3 ] DiffOK:[4 ] MinLEN:[9 ]
           Digits: [-1 ] Upper: [-1 ] Lower: [-1 ] Other:[-1 ]

< Update >

Help: <F1> // Exit: ^Q or ^C // Menus (Top-bar): ^X

```

Figure 283 Configuring Password Settings

Select either **Regular**, **Random**, or **Strong** for the **admin** and **status** (if enabled) passwords.

PASSWORD SETTING	DESCRIPTION
Regular	These are standard, yet a fairly weak password system. Passwords have to be longer than 4 characters with few restrictions. This is the system default password configuration.
Random	Provides randomly-generated passwords. Configure the maximum password size in bits (minimum is 14, maximum is 70, default is 20) and number of retries (default is 10), which is the number of times you will be asked if you want to accept the new password. You can either accept (by typing in the new password twice) or reject the random password. You cannot select your own password.
Strong	Enforce strong passwords. Retries is the number of times you are prompted before an error message is issued. DiffOK means how many characters can be the same in the new password relative to the old. MinLEN is the minimum length of characters required in the password. Specify how many Digits, Upper-case letters, Lower-case letters, and Other (special) characters are required in the password. Positive numbers indicate the maximum amount of “credit” of this character class can be accrued towards the “simplicity” count. Negative numbers implies that the password MUST have at least that many characters from this given class. Thus, numbers of -1 means that every password must have at least one digit in it.

Account Configuration

By default, the **status** account does not require a password, but you can configure it to have one here. Other aspects of the admin password can be configured and the Field Support accounts can be enabled or disabled.

1. To configure accounts, click **Operation**, **Admin**, **Change Passwords**, then **Account Configuration**.

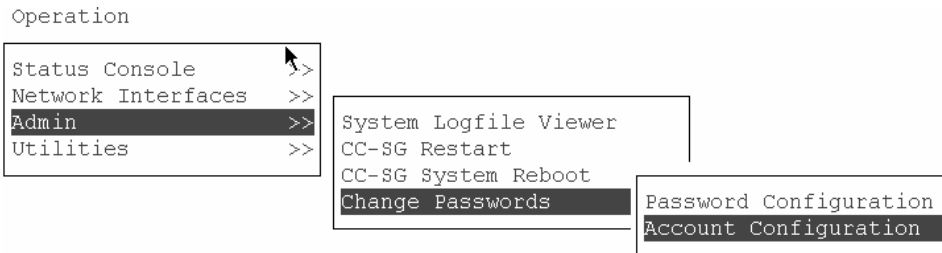


Figure 284 Account Configuration

2. View the settings for each account, that is **Status**, **Admin**, **FS1** and **FS2**.

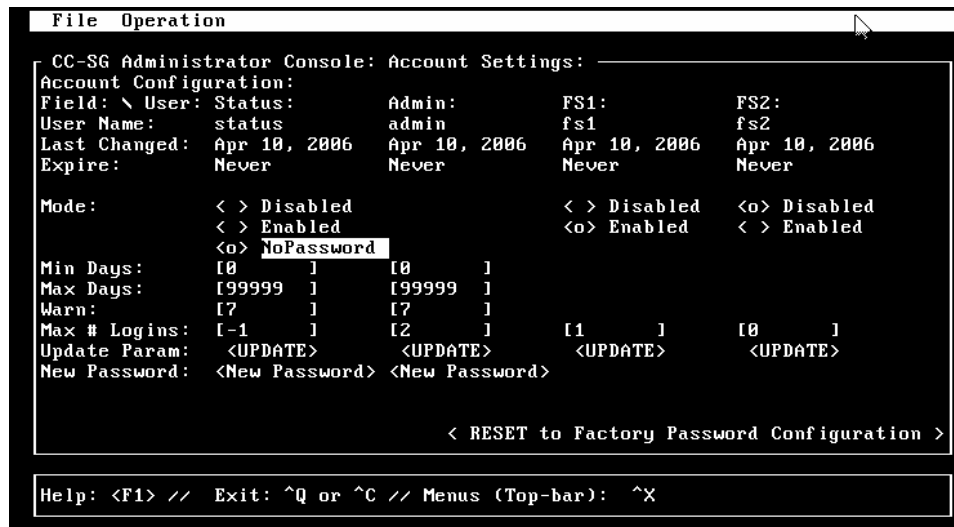


Figure 285 Configuring Accounts

3. If you want to require a password for the **Status** account, select **Enabled** underneath it.

This screen is split into three main areas:

- The top displays read-only information about the accounts on the system.
- The middle section displays the various parameters related and pertinent to each ID, along with a set of buttons, to allow the parameters to be updated or new passwords provided for the accounts.
- The final area restores the password configuration to Factory Defaults (or how the system was initially shipped).

4. For the **Admin** and **Status** accounts, you can configure:

SETTING	DESCRIPTION
User \ User Name	This is the current user name or ID for this account. (This may be operator changeable in a future release.)
Last Changed	(Read-only). This is the date of the last password change for this account.
Expire	(Read-only). Tells the day that this account must change its password.
Mode	A configurable option if the account is disabled (no login allowed), or enabled (authentication token required), or access is allow and no password is required. (Great care should be taken to make certain that both the Admin and FS1 accounts are not locked out at the same time; otherwise, you may not be able to use Diagnostic Console.)
Min Days	The minimum number of days after a password has been changed before it can be changed again. Default is 0 .
Max Days	The maximum number of days the password will stay in affect. Default is 99999 .
Warning	The number of days that warning messages are issued before the password expires. Warning messages are hard to see in a forms-based system like Diagnostic Console.
Max # of Logins	The maximum number of concurrent logins the account will allow. Negative numbers indicate no restrictions (-1 is the default for status login). 0 means no one can log in. A positive number defines the number of concurrent users who can be logged in (2 is the default for admin login).
Update Param	Install any changes for this ID that have been made.
New Password	Enter a new password for the account.

Displaying Disk Status (Utilities)

This option displays status of CC-SG disks, such as size of disks, if they are active and up, and amount of space currently used by various file systems.

- To display disk status of the CC-SG, click **Operation**, **Utilities**, then **Disk Status**.

Operation

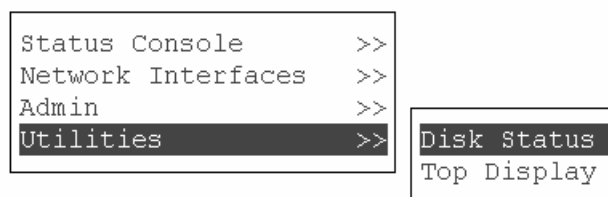


Figure 286 Selecting Disk Status in Diagnostic Console

2. Either click **Refresh** or press **Enter** to refresh the display. Refreshing the display is especially useful when upgrading or installing and you want to see the progress of the RAID disks as they are being rebuilt and being synchronized.

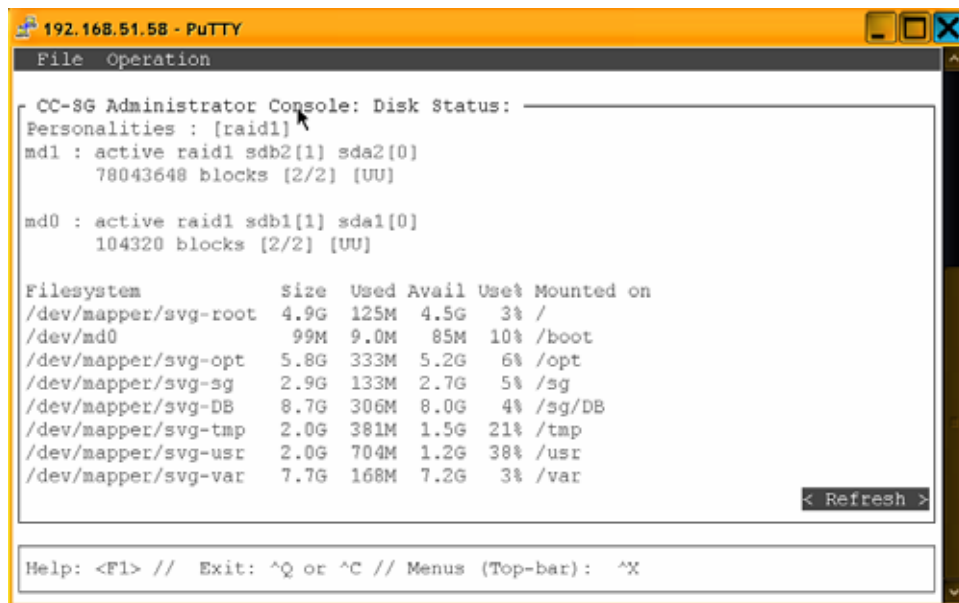


Figure 287 Displaying Disk Status of CC-SG in Diagnostic Console

The disk drives are fully synchronized and full RAID-1 protection is available when you see a screen as shown above (note the status of both **md0** and **md1** arrays are [UU]).

Displaying Top Display (Utilities)

This option displays the list of processes and their attributes that are currently running on CC-SG as well as overall system health.

1. To display the processes running on the CC-SG, click **Operation**, **Utilities**, then **Top Display**.



Figure 288 Selecting Top Display in Diagnostic Console

2. View the total running, sleeping, total number and processes that have stopped.

```

top - 12:08:26 up 3 days, 20:43, 1 user, load average: 0.08, 0.24, 0.43
Tasks: 95 total, 2 running, 93 sleeping, 0 stopped, 0 zombie
Cpu(s): 3.0% us, 3.7% sy, 0.0% ni, 93.3% id, 0.0% wa, 0.0% hi, 0.0% si
Mem: 2076084k total, 1335452k used, 740632k free, 245096k buffers
Swap: 2031608k total, 0k used, 2031608k free, 511344k cached

  PID USER      PR  NI  VIRT  RES  SHR  S  %CPU  %MEM    TIME+  COMMAND
 25934 postgres 15   0 22508 9960 8744  S   1.7   0.5   0:02.25 postmaster
 22990 postgres 15   0 22504 13m 12m  S   1.3   0.7   1:11.28 postmaster
  2103 root      18   0 6100 3396 1752  S   0.3   0.2   10:08.61 status-poller.p
  2891 sg       16   0 2808 1500 1156  S   0.3   0.1   0:41.26 rarvendd
    1 root     16   0 3460 552 476  S   0.0   0.0   0:00.84 init
    2 root     34  19   0   0   0  S   0.0   0.0   0:00.09 ksoftirqd/0
    3 root      5 -10   0   0   0  S   0.0   0.0   0:00.01 events/0
    4 root      5 -10   0   0   0  S   0.0   0.0   0:00.01 khelper
    5 root     15 -10   0   0   0  S   0.0   0.0   0:00.00 kacpid
   25 root      5 -10   0   0   0  S   0.0   0.0   0:00.00 kblockd/0
   35 root     20   0   0   0   0  S   0.0   0.0   0:00.00 pdflush
   36 root     15   0   0   0   0  S   0.0   0.0   0:02.12 pdflush
   38 root     13 -10   0   0   0  S   0.0   0.0   0:00.00 aio/0
   26 root     15   0   0   0   0  S   0.0   0.0   0:00.00 khubd
   37 root     25   0   0   0   0  S   0.0   0.0   0:00.00 kswapd0
  111 root     25   0   0   0   0  S   0.0   0.0   0:00.00 kseriod
  176 root      5 -10   0   0   0  S   0.0   0.0   0:00.00 ata/0
  
```

Figure 289 Displaying CC-SG Processes in Diagnostic Console

3. Type **h** to bring up an extensive help screen for the top command. The standard **F1** help key is not operational at this point. To return to the Admin Console, use the standard **CTL+Q** or **CTL+C**.

Appendix A: Specifications (G1, V1)

G1 Platform

General Specifications

Form Factor	1U
Dimensions (DxWxH)	22.1"x 17.32" x 1.75" 563mm x 440mm x 44mm
Weight	24.07lb (10.92kg)
Power	Redundant, hot-swappable power supplies, auto-sensing 110/220 V – 2.0A
Mean Time Between Failure (MTBF)	38,269 hours
KVM Admin Port	(DB15 + PS2 Keyboard/Mouse)
Serial Admin Port	DB9
Console Port	N/A

Hardware Specifications

Processor	Intel® Pentium® III 1 GHz
Memory	512 MB
Network Interfaces	(2) 10/100 Ethernet (RJ45)
Hard Disk & Controller	(2) 40-GB IDE @7200 rpm, RAID 1
CD-ROM Drive	CD-ROM 40x Read Only
IPMI	N/A

Remote Connection

Modem	V.92 (56Kbps); RJ-11 connector
Protocols	TCP/IP, UDP, RADIUS, LDAP, TACACS+, SNMP, SNTP, HTTP, HTTPS
Warranty	Two years with Advanced Replacement* Guardian Extended Warranty Also Available

Environmental Requirements

OPERATING	
Humidity	20% - 85% RH
Altitude	Operate properly at any altitude between 0 to 10,000 feet, storage 40,000 feet (est.)
Vibration	5-55-5 HZ, 0.38mm, 1 minutes per cycle; 30 minutes for each axis (X, Y, Z)
Shock	N/A

NON-OPERATING	
Temperature	0 - 30 deg C; 32 – 104 deg F
Humidity	10% - 90% RH
Altitude	Operate properly at any altitude between 0 to 10,000 feet, storage 40,000 feet (est.)
Vibration	5-55-5 HZ, 0.38mm, 1 minutes per cycle; 30 minutes for each axis (X, Y, Z)
Shock	N/A

Electrical Specifications

INPUT	
Nominal Frequencies	50/60 Hz
Nominal Voltage Range	100/240 VAC
Maximum Current AC RMS	2A
AC Operating Range	100 to 240 VAC (+-10%), 47 to 63 Hz
OUTPUT	
+5 VDC, +12VDC	N/A
-5 VDC, -12VDC	N/A
Maximum DC Power Output	N/A
Maximum AC Power Consumption	N/A
Maximum Heat Dissipation	N/A
Volt-Ampere Rating	N/A

V1 Platform

General Specifications

Form Factor	1U
Dimensions (DxWxH)	24.21" x 19.09" x 1.75" 615mm x 485mm x 44mm
Weight	23.80lb (10.80kg)
Power	Single Supply (1 x 300 watt)
Operating Temperature	10°C- 35°C (50°F- 95°F)
Mean Time Between Failure (MTBF)	36,354 hours
KVM Admin Port	(DB15 + PS2 or USB Keyboard/Mouse)
Serial Admin Port	DB9
Console Port	2 x USB 2.0 Ports

Hardware Specifications

Processor	AMD Opteron 146
Memory	2 GB
Network Interfaces	(2) 10/100/1000 Ethernet (RJ45)
Hard Disk & Controller	(2) 80-GB SATA @ 7200 rpm, RAID 1
CD-ROM Drive	DVD-ROM

Remote Connection

Modem	Not Applicable
Protocols	TCP/IP, UDP, RADIUS, LDAP, TACACS+, SNMP, SNTP, HTTP, HTTPS
Warranty	Two years with Advanced Replacement* Guardian Extended Warranty Also Available

Environmental Requirements

OPERATING	
Humidity	8% - 90% RH
Altitude	Operate properly at any altitude between 0 to 10,000 feet, storage 40,000 feet (Estimated)
Vibration	5-55-5 HZ, 0.38mm, 1 minutes per cycle; 30 minutes for each axis(X,Y,Z)
Shock	N/A

NON-OPERATING	
Temperature	-40° - +60° (-40°-140°)
Humidity	5% - 95% RH
Altitude	Operate properly at any altitude between 0 to 10,000 feet, storage 40,000 feet (Estimated)
Vibration	5-55-5 HZ, 0.38mm, 1 minutes per cycle; 30 minutes for each axis (X,Y,Z)
Shock	N/A

Electrical Specifications

INPUT	
Nominal Frequencies	50/60 Hz
Nominal Voltage Range	100/240 VAC
Maximum Current AC RMS	3A
AC Operating Range	100 to 240 VAC (+-10%), 50/60 Hz
OUTPUT	
+5 VDC, +12VDC	N/A
-5 VDC, -12VDC	N/A
Maximum DC Power Output	N/A
Maximum AC Power Consumption	Average Power Consumption: 249.7 – 250.8 Watts Max. Power Consumption: 250.8 Watts
Maximum Heat Dissipation	Average Heating Value: 214.74k – 215.69k cal Max. Heating Value: 215.69k cal
Volt-Ampere Rating	N/A

Appendix B: CC-SG and Network Configuration

Introduction

This appendix discloses network requirements (addresses, protocols and ports) of a typical CommandCenter Secure Gateway (CC-SG) deployment. It provides what you need to know and how to configure your network for both external access (if desired) and internal security and routing policy enforcement (if used). Details are provided for the benefit of a TCP/IP network administrator, whose role and responsibilities may extend beyond that of a CC-SG administrator and who may wish to incorporate CC-SG and its components into site's security access and routing policies.

As depicted in the diagram below (see Figure #1), a typical CC-SG deployment may have none, some, or all of the features, for example, a firewall or a Virtual Private Network (VPN). The tables that follow disclose the protocols and ports that are needed by CC-SG and its associated components, which are essential to understand especially if firewalls or VPNs are present in your network and access and security policies are to be enforced by the network.

Executive Summary

In the sections below, a very complete and thorough analysis of the communications and port usage by CC-SG and its associated components is provided. For those customers that just want to know what ports to open on a firewall to allow access to CC-SG and the targets that it controls, the following ports should be opened:

Port Number	Protocol	Purpose
80	TCP	HTTP Access to CC-SG
443	TCP	HTTPS (SSL) Access to CC-SG
8080	TCP	CC-SG <-> PC Client
2400	TCP	Target Access (Proxy Mode & In-Band Access)
5000 ¹	TCP	Target Access (Direct Mode)
51000 ¹	TCP	SX Target Access (Direct Mode)

This list can be further trimmed:

- Port 80 can be dropped if all access to the CC-SG is via HTTPS addresses.
- Ports 5000 and 51000 can be dropped if CC-SG Proxy mode is used for any connections from the firewall(s).

Thus, a minimum configuration only requires three (3) ports [443, 8080, and 2400] to be opened to allow external access to CC-SG.

In the sections below, the details about these access methods and ports are provided along with configuration controls and options.

¹ These ports need to be opened per Raritan device that will be externally accessed. The other ports in the table need to be opened only for accessing CC-SG.

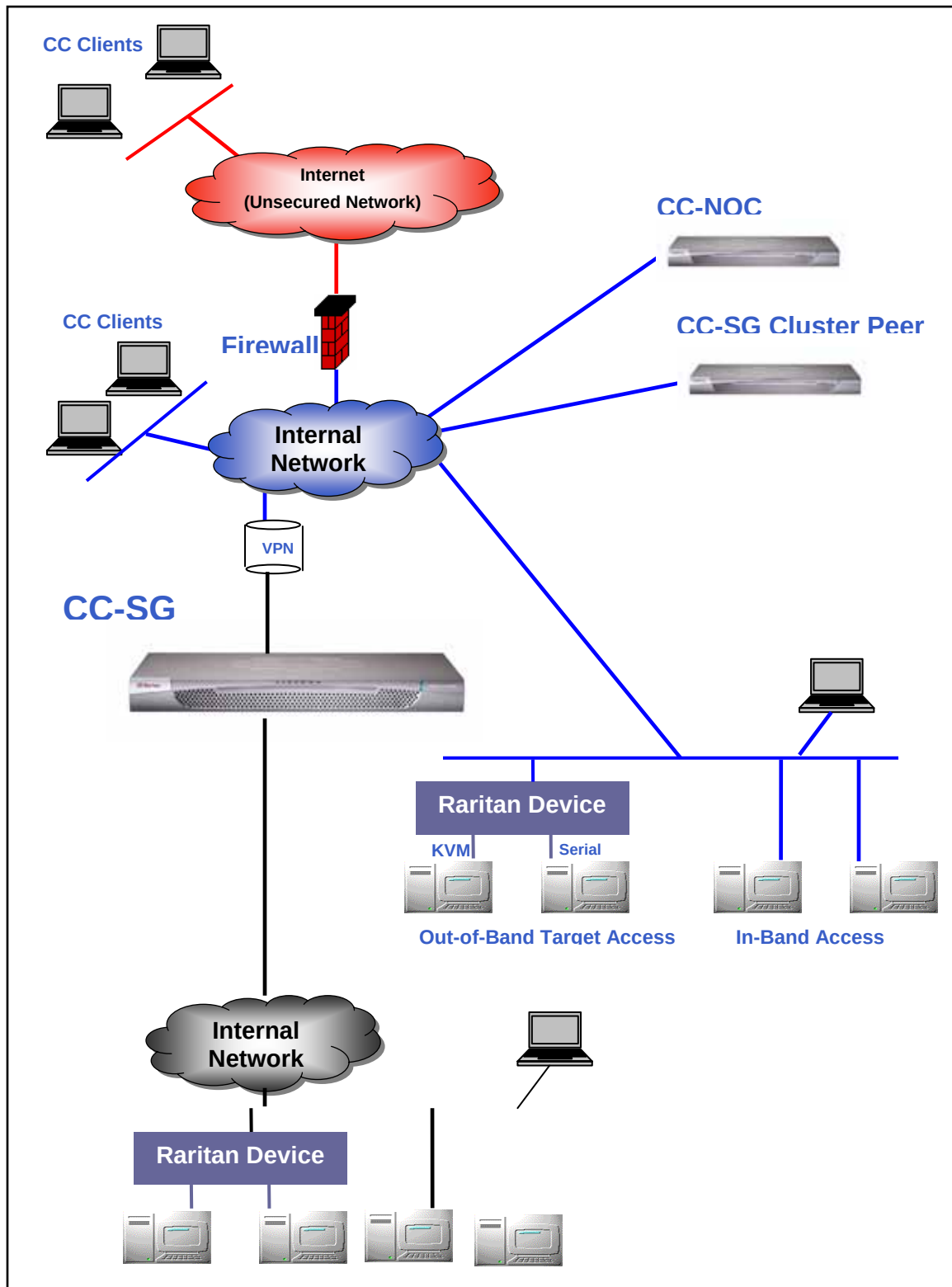


Figure 290 CC-SG Deployment Elements

CC-SG Communication Channels

The communication channels are partitioned as follows:

- CC-SG ↔ Raritan Devices
- CC-SG ↔ CC-SG Clustering (optional)
- CC-SG ↔ Infrastructure Services
- Clients ↔ CC-SG
- Clients ↔ Targets (Direct Mode)
- Clients ↔ Targets (Proxy Mode)
- Clients ↔ Targets (In-Band)
- CC-SG ↔ CC-NOC

For each communication channel, the tables in the sections that follow:

- Represents the symbolic **IP Addresses** used by the communicating parties. These addresses have to be allowed over any communication path between the entities.
- Indicates the **Direction** in which the communication is initiated. This may be important for your particular site policies. For a given CC-SG role, the path between the corresponding communicating parties must be available and for any alternate re-route paths that might be used in the case of a network outage.
- Provides the **Port Number** and **Protocol** used by CC-SG.
- States the **Purpose** of the port.
- Indicates if the port is **Configurable**, which means the GUI or Diagnostic Console provides a field where you can change the port number to a different value from the default listed due to conflicts with other applications on the network or for security reasons.

CC-SG and Raritan Devices

A main role of CC-SG is to manage and control Raritan devices (for example, Dominion KX, KSX, etc.). Typically, CC-SG communicates with these devices over a TCP/IP network (local, WAN, or VPN) and both TCP and UDP protocols are used as follows:

Communication Direction	Port Number	Protocol	Purpose	Configurable?
CC-SG → Local Broadcast	5000	UDP	Device Discovery	yes
CC-SG → Remote LAN IP	5000	UDP	Device Discovery	yes
CC-SG → Raritan Device	5000	TCP	Device Control	yes
Raritan Device → CC-SG	5001	UDP	Device Events	no

CC-SG Clustering

When the optional CC-SG clustering feature is used (that is, two CC-SGs are inter-connected and function as one unit), the following ports must be available for the inter-connecting sub-networks. {If the optional clustering feature is not used, none of these ports need to be made available in the network.}

Each CC-SG in the cluster may be on a separate LAN. However, the inter-connection between the units should be very reliable and not prone to periods of congestion.

Communication Direction	Port Number	Protocol	Purpose	Configurable?
CC-SG → Local Broadcast	10000	UDP	CC-SG Discovery	no
CC-SG → Remote LAN IP	10000	UDP	CC-SG Discovery	no
CC-SG ↔ CC-SG	5432	TCP	DataBase Replication	no
CC-SG ↔ CC-SG	8732	TCP	Cluster Heartbeat	no
CC-SG ↔ CC-SG	3232	TCP	SNMP	no

Access to Infrastructure Services

The CC-SG can be configured to use several industry-standard services like DHCP, DNS, and NTP. In order for CC-SG to communicate with these optional servers, these ports and protocols are used:

Communication Direction	Port Number	Protocol	Purpose	Configurable?
DHCP Server → CC-SG	68	UDP	DHCP Lease	no
CC-SG → DHCP Server	67	UDP	DHCP Request	no
NTP Time Server ↔ CC-SG	123	UDP	Time Updates	no
CC-SG → DNS	53	UDP	Name Server Queries	no

PC Clients to CC-SG

PC Clients connect to the CC-SG in one of these three modes:

- Web / Java Applet CC-SG GUI interface
- CC-SG Command Line Interface via SSH
- CC-SG Diagnostic Console

The first mode is the primary means for users and administrators to connect to CC-SG. The other two modes are less frequently used. These modes require the following networking configuration:

Communication Direction	Port Number	Protocol	Purpose	Configurable?
Client → CC-SG GUI	443	TCP	HTTPS Access	no
Client → CC-SG GUI	80	TCP	HTTP Access (redirect to HTTPS)	no
Client → CC-SG GUI	8080	TCP	Tomcat Access	no
Client → CC-CLI SSH	22	TCP	CC-SG CLI	yes
Client → CC Diagnostic Console	23	TCP	Status and Maintenance	yes

PC Clients to Targets

Another significant role of CC-SG is to connect PC clients to various targets (or endpoints). These targets can be serial or KVM console connections to Raritan devices (called Out-of-Band connections). Another mode is to use In-Band access (IBA) methods, for example, Virtual Network Computer (VNC), Windows Remote Desktop (RDP), or Secure Shell (SSH).

Another facet of PC client to target communication is whether:

- The PC client connects directly to the target (either via a Raritan device or In-Band access), which is called **Direct Mode**.
- Or, if the PC client connects to the target through CC-SG, which acts as an application firewall and is called **Proxy Mode**.

Communication Direction	Port Number	Protocol	Purpose	Configurable?
Client → CC-SG via Proxy → Target	2400 (on CC-SG)	TCP	Proxy Mode	no
Client → Raritan Target (Direct Mode)	5000 (on device)	TCP	Raritan Direct	yes
Client → Dominion SX → (Direct Mode)	51000	TCP	Target Access	yes

CC-SG & Client for IPMI, iLO/RILOE, Etc.

Another significant role of CC-SG is to manage third-party devices, such as iLO/RILOE, Hewlett Packard's Integrated Lights Out/Remote Insight Lights Out servers. Targets of an iLO/RILOE device are powered on/off and recycled directly. Intelligent Platform Management Interface (IPMI) servers can also be controlled by CC-SG.

Communication Direction	Port Number	Protocol	Purpose	Configurable?
CC-SG → IPMI	623	UDP	Device Discovery	yes
CC-SG → iLO/RILOE (uses HTTP ports)	80 or 443	UDP	Device Discovery	no

CC-SG & SNMP

Simple Network Management Protocol (SNMP) allows CC-SG to push SNMP traps (event notifications) to an existing SNMP manager on the network. CC-SG also supports SNMP GET/SET operations with third-party Enterprise Management Solutions, such as HP OpenView.

Communication Direction	Port Number	Protocol	Purpose	Configurable?
SNMP Manager → CC-SG	161	UDP	SNMP Get, Set	yes
CC-SG → SNMP Manager	162	UDP	Sending Traps	yes

CC-SG & CC-NOC

CC-NOC is an optional appliance that can be deployed in conjunction with CC-SG. CC-NOC is a Raritan network-monitoring appliance that audits and monitors the status of servers, equipment, and Raritan devices that CC-SG manages.

Communication Direction	Port Number	Protocol	Purpose	Configurable?
CC-SG ↔ CC-NOC	9443	TCP	CC-SG, CC-NOC Communications	no

CC-SG Internal Ports

CC-SG uses several ports for internal functions and its local firewall function blocks access to these ports. However, some external scanners may detect these as “blocked” or “filtered”. External access to these ports is not required and can be further blocked. The ports currently in use are:

1088, 1098, 2222, 4444, 4445, 8009, 8083 and 8093

In addition to these ports, CC-SG may have a couple of TCP and UDP ports in the 32xxx (or higher) range open. External access to these ports is not required and can be blocked.

CC-SG Access via NAT-enabled Firewall

If the firewall is using NAT (Network Address Translation) along with possibly Port Address Translation (PAT), then Proxy mode should be used for all connections that use this firewall. Moreover, the firewall must be configured for external connections to Ports 80(non-SSL)/443(SSL)², 8080 and 2400 to be forwarded to CC-SG (since the PC Client will initiate sessions on these ports).

All In-Band Access (IBA) connections use the CC-SG as the Proxy connection and no additional configuration is required. Out-of-Band Access (OBA) connections using the firewall must be configured on the **Setup → Configuration Manager → Connection Mode** menu to use Proxy mode. This way, CC-SG will connect to the various targets (either IBA or OBA) on behalf of the PC Client requests. However, the CC-SG will terminate the PC Client to Target TCP/IP connection that comes through the firewall.

² It is NOT recommended to run non-SSL traffic through a firewall.

Security and Open Port Scans

As part of the CC-SG Quality Assurance process, several open port scanners are applied to the product and Raritan Computer makes certain that its product is not vulnerable to these known attacks. All the open or filtered/blocked ports are listed in the above sections. Some of the more common exposures are:

Issue ID ³	Synopsis	Comment
CVE-1999-0517 CVE-1999-0186 CVE-1999-0254 CVE-1999-0516	snmp (161/UDP) - the community name of the remote SNMP server can be guessed.	Default CC-SG SNMP community name is “public”. Users are encouraged to change this to the site-specific value (Setup → Configuration Manager → SNMP menu). Please refer to the CC-SG Administrator Guide for more additional information.
CVE-2000-0843	The remote telnet server shut the connection abruptly when given a long username followed by a password.	Traditionally, port 23 is used for telnet services. However, CC-SG uses this port for SSH V2 Diagnostic Console sessions. Users may change the port and/or completely disable Diagnostic Console from using the SSH Access method. Please refer to the CC-SG Administrator Guide for more additional information.
CVE-2004-0230	The remote host might be vulnerable to a sequence number approximation bug, which may allow an attacker to send spoofed RST packets to the remote host and close established connections.	The underlying TCP/IP protocol stack used by CC-SG has not been shown to be susceptible to this exposure.
CVE-2004-0079 CVE-2004-0081 CVE-2004-0112	The remote host is using a version of OpenSSL which is older than 0.9.6m or 0.9.7d.	The following patches have been applied to OpenSSL, therefore removing this exposure: • RHSA-2004:120 • RHSA-2005:830. • RHSA-2003:101-01

³ CVEs can be found on <http://cve.mitre.org>.

Appendix C: Initial Setup Process Overview

Pre-requisites:

- Add Devices with Category/Element clearly identified.
- Add Ports with Category/Element clearly identified.

Create Group(s)/Add User(s)

1. Add Device Group with rule based on Category/Element
2. Add Port Group with rule based on Category/Element
3. Add Policy (links 2 and 3 together; controls access time and permission)
4. Link Groups/Users to Policy of choice

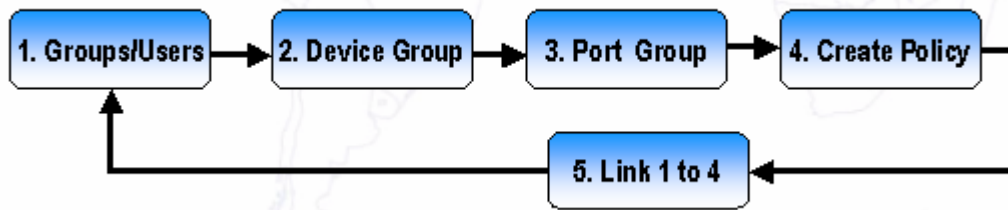


Figure 291 Association Management Process

Appendix D: User Group Privileges

USERS GROUP PRIVILEGE	AVAILABLE COMMANDS	USER CAPABILITY
CC Setup And Control	Application Manager	Users are able to add new application to CC-SG.
	Security Manager	Users are able to configure security parameters.
	Configuration Manager	Users are able to make general configuration of CC-SG.
	Restart CommandCenter	Users are able to restart CC-SG.
	Shutdown CommandCenter	Users are able to shutdown CC-SG.
	Backup CommandCenter	Users are able to backup CC-SG database.
	Restore CommandCenter	Users are able to restore a previous backup of CC-SG.
	Reset CommandCenter	Users are able to factory reset CC-SG.
	Upgrade CommandCenter	Users are able to upgrade CC-SG.
	Cluster Configuration	Users are able to configure cluster of CC-SG.
	User data	Users are able to view “User data” report.
	CommandCenter NOC	Users are able to view and configure “CommandCenter NOC” parameters
	Cross Compatibility Matrix	Users are able to view “Compatibility Matrix”.
Device Configuration And Upgrade Management	Backup Device Configuration	Users are able to perform back up of device configuration.
	Restore Device Configuration	Users are able to perform restore device configuration.
	Copy Device Configuration	Users are able to copy device configuration.
	Ping Device	Users are able to ping other devices.
	Restart Device	Users are able to restart other devices.
	Pause/Resume Device Management	Users are able to release device from CC-SG control.
	Upgrade Device	Users are able to upgrade device.
	Firmware Manager	Users are able to upload firmware files for devices.
	Devices Tree	Users are able to view devices tree.
	Cross Compatibility Matrix	Users are able to view “Compatibility Matrix”.
	Ping Report	Users are able to view ping report.
	Active Ports	Users are able to view active ports report.
	User data	Users are able to view “User data” report.

USERS GROUP PRIVILEGE	AVAILABLE COMMANDS	USER CAPABILITY
Device And Port Management	Configuration Manager	Users are able to change general device settings configuration of CC-SG.
	Add Device	Users are able to add new devices.
	Edit Device	Users are able to modify devices name and parameters.
	Delete Device	Users are able to delete devices.
	Bulk Device Copy	Users are able to copy device parameters to other devices.
	Ping Device	Users are able to ping other devices.
	Restart Device	Users are able to restart other devices.
	Pause/Resume Device Management	Users are able to release device from CC-SG control.
	Topological View	Users are able to display the actual topology of devices.
	Device Power Manager	Users are able to turn on and off devices.
	Discover Raritan Devices	Users are able to manually discover Raritan devices.
	Change Port View	Users are able to customize port view.
	Edit Port	Users are able to modify port name and parameters.
	Active Ports	Users are able to view active ports report.
	Asset Management Report	Users are able to view asset management report.
	Ping Report	Users are able to view ping report.
	Query Port	Users are able to view report of ports.
	Port/Device Trees	Users are able to view ports and devices tree.
	CommandCenter NOC	Users are able to view and configure “CommandCenter NOC” parameters
	Port Sorting	Users are able to sort ports visible in Ports/Devices Tree.
	Compatibility Matrix	Users are able to view “Compatibility Matrix”.
	Disconnect Users	Users are able to disconnect SX locally connected users.
Ports Access	Connect Port	Users are able to see port and connect to it.
	Disconnect Port	Users are able to see port and disconnect it.
	Port Power Manager	Users are able to turn on and off a port.
	Change Port View	Users are able to customize port view.
	Ports Tree	Users are able to view ports tree.
	Active Ports	Users are able to view “Active Ports” report for own ports connected.
	User data	Users are able to view “User data” report.
	Port Sorting	Users are able to sort ports visible in Ports Tree.

USERS GROUP PRIVILEGE	AVAILABLE COMMANDS	USER CAPABILITY
User Security Management *Note that this privilege is not configurable and is only assigned to the System Administrator user group by default.	Association Manager	Users are able to associate categories and elements.
	Device Group Manager	Users are able to rename groups and add rules to device groups.
	Port Group Manager	Users are able to rename groups and add rules to port groups.
	Policy Manager	Users are able to add and edit policies.
	Edit User Group Policies	Users are able to modify and assign policies to groups.
	Group Data	Users are able to view group parameters.
	Users Tree	Users are able to view users tree.
User Management *Note that this privilege is not configurable and is only assigned to the System Administrator user group by default.	Add User	Users are able to add user to the system.
	Edit User	Users are able to modify user name and parameters.
	Change User Password	Users are able to change other user password.
	Delete User	Users are able to delete user from the system.
	Logoff User	Users are able to logoff user.
	Bulk User Copy	Users are able to copy user's parameters.
	Add User To Group	Users are able to add user to a group.
	Delete User From Group	Users are able to delete user from group.
	Add User Group	Users are able to add user group.
	Edit User Group	Users are able to modify user group name and parameters.
	Delete User Group	Users are able to delete user group.
	Assign Users To Group	Users are able to assign users from other groups.
	Active Users	Users are able to view active ports.
	Users Data	Users are able to view users parameters.
	Users In Groups	Users are able to view users logged in the system.
	Users Tree	Users are able to view users tree.

Appendix E: SNMP Traps

CC-SG provides the following traps:

SNMP TRAP	DESCRIPTION
CCDeviceUpgrade	CC-SG has upgraded the firmware on a device.
CCImageUpgradeResults	CC-SG image upgrade results.
CCImageUpgradeStarted	CC-SG image upgrade started.
CCIncompatibleDeviceFirmware	CC-SG detected device with incompatible firmware.
CCLeafNodeAvailable	CC-SG detected leaf node reachable.
CCLeafNodeUnavailable	CC-SG detected a connection failure to a leaf node.
CCPortConnectionStarted	CC-SG session started.
CCPortConnectionStopped	CC-SG session stopped.
CCPortConnectionTerminated	CC-SG session terminated.
CCRootPasswordChanged	CC-SG root password changed.
CCUserAdded	CC-SG - a new user added.
CCUserAuthenticationFailure	CC-SG user authentication failure.
CCUserDeleted	CC-SG - a user deleted.
CCUserLogin	CC-SG user Log in.
CCUserLogout	CC-SG user Log out.
CCUserModified	CC-SG user modified.
CCAvailable	CC-SG application is available.
CCDeviceAddedAfterCCNOCNotification	CC-SG device added after NOC notification.
CCDiagnosticConsole	CC-SG user logged into Diagnostic Console.
CCDiagnosticConsoleLogout	CC-SG locked out user from login.
CCEnterMaintenanceMode	CC-SG entered maintenance mode.
CCExitMaintenanceMode	CC-SG exited maintenance mode.
CCHardDiskFailure	CC-SG detected a hard disk failure.
CCLanCardFailure	CC-SG detected a LAN card failure.
CCNOCAvailable	CC-SG detected that CC-NOC is available.
CCNOCUnavailable	CC-SG detected that CC-NOC is unavailable.
CCScheduledTaskExecutionFailure	CC-SG failed to execute scheduled task.
CCUnavailable	CC-SG application is unavailable.
CCUserLockedOut	CC-SG locked out user from login.

Appendix F: Troubleshooting

- In order to launch CC-SG from your web browser, it requires a Java plug-in. If your machine has an incorrect version, CC-SG will guide you through the installation steps. If your machine does not have a Java plug-in, CC-SG cannot automatically launch. In this case, you must uninstall or disable your old Java version and provide serial port connectivity to CC-SG to ensure proper operation.
- If the CC-SG applet does not load, check your Web browser settings.
 - In IE: on the Tools menu, click Internet Options and click on the Advanced tab. Ensure Java (Sun) is enabled.
 - Open Java Plug-in in your Control Panel, click on the Browser tab, and adjust the settings for your browser.
- If you have problems adding devices, ensure the devices have the correct firmware versions.
- If the network interface cable is disconnected between the device and CC-SG, wait for the configured heartbeat minutes and then plug the network interface cable back in. During the configured heartbeat period, the device operates in standalone mode and can be accessed through RRC, MPC, RC, etc.
- If you receive an error message that states your client version is different from the server version and that behavior may be unpredictable, you should restart or empty the cache of your browser.

Client Browser Requirements

Please see your CC-SG Compatibility Matrix for the most current matrix of Client Browser and PC Platform Requirements.

Go to <http://www.raritan.com/support> and click **Firmware Upgrades**, then **CommandCenter**.

Import CSV File (Category, Device, Port) Error Message

If you receive a “No valid element was found in the analysed file” error message or “Element ‘Category’ not found in definition” message, remove the “” from the CSV file. Please see Chapter 4: Creating Associations for additional information.

Port and Policy Group Creation Failure

The default port groups and policies created in the Association Wizard are named after the elements of a category. If the element names are not unique, the default port groups and policies cannot be created (see the screen below) and will appear in red. Rename the elements of the category so they are unique.

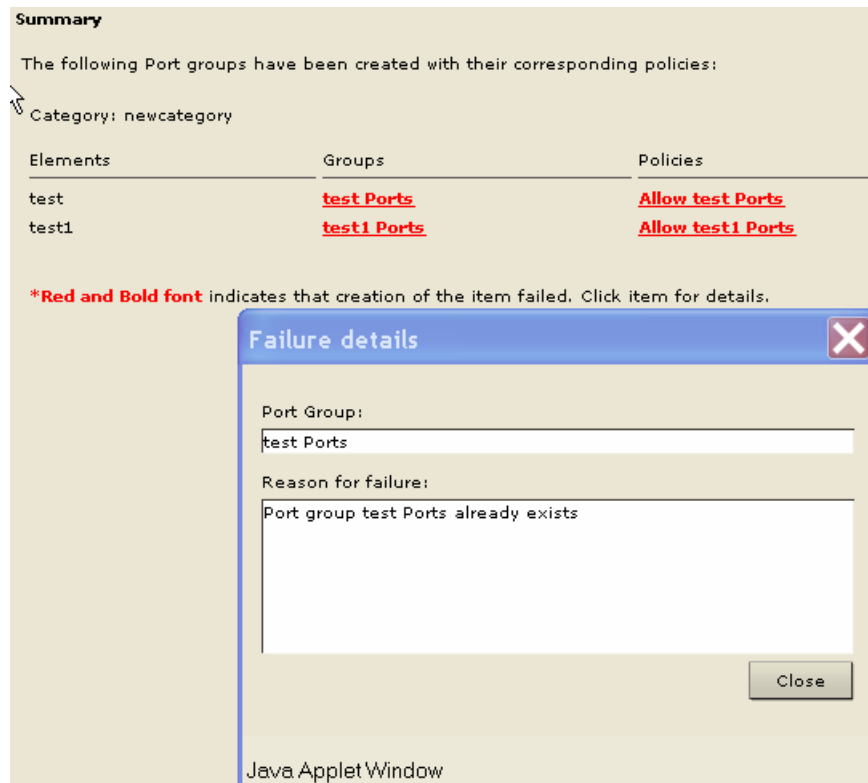


Figure 292 Port Group Failure

Appendix G: FAQs

QUESTION	ANSWER
General	
What is CC-SG?	CC-SG is a network management device for aggregating and integrating multiple servers and network equipment typically deployed in a datacenter and which are connected to a Raritan IP-enabled product.
Why would I need CC-SG?	As you deploy more and more datacenter servers and devices, their management becomes exponentially complex. CC-SG allows a systems administrator or manager to access and manage all servers, equipment, and users from a single device.
What is CommandCenter NOC?	CommandCenter NOC is a network monitoring device for auditing and monitoring the status of servers, equipment and Raritan devices that CC-SG provides access to.
Which Raritan products does CC-SG support?	CC-SG supports all Dominion products - Raritan's KVM over IP products - Dominion KX - Raritan's Secure Console Server products - Dominion SX - Raritan's Remote office management products - Dominion KSX CC-SG also supports Paragon II when used with the optional IP user stations.
How does CC-SG integrate with other Raritan Products?	CC-SG uses a unique and proprietary search and discovery technology that identifies and connects to selected Raritan devices with a known network address. Once CC-SG is connected and configured, the devices connected to CC-SG are transparent, and operation and administration is extremely simple.
Is PDA access possible?	Generic answer: "Yes", as long as PDA has a Java-enabled browser and supports 128-bit (or lower strength for some geographies) SSL encryption. Call Raritan Tech Support for further information. No testing has been done in this area.
Is the status of CC-SG limited by the status of the devices which it proxies?	No. Because CC-SG software resides on a dedicated server, even if a device being proxied by the CC-SG is turned off, you will still be able to access CC-SG.
Can I upgrade to newer versions of CC-SG software as they become available?	Yes. Contact your authorized Raritan sales representative or Raritan, Inc. directly. CC-SG 2.0 has a CD-ROM drive to facilitate upgrades. New version upgrades can also be done via FTP.
How many target devices (ports) and/or Dominion units and/or IP-Reach units can be connected to CC-SG?	There is no specified limit to the number of ports and/or Dominion and/or IP-Reach units that can be connected, but the number is not limitless: the performance of the processor and the amount of memory on the hosting server will determine how many ports can actually be connected.
Is there any way to optimize the performance of Microsoft Internet Explorer if it is my preferred Web browser?	To improve the performance of Microsoft IE when accessing the console, disable the "JIT compiler for virtual machine enabled," "Java logging enabled," and "Java console enabled" options. From the main menu bar, select Tools > Internet Options > Advanced . Scroll down until you see the above items and make sure that they are not checked.
What do I do if I am unable	Assuming the console/serial device is a Dominion, ensure that

QUESTION	ANSWER
to add a console/serial port to CC-SG?	the following conditions are met: - The Dominion unit is active. - The Dominion unit has not reached the maximum number of configured user accounts.
Which version of Java will Raritan's CC-SG be supporting?	The earliest version CC-SG will support will be at least the Java 2 platform. Users must download the Java 2 plug-in if using IE. By default, Netscape will use Sun JVM. For server and client side minimum Java requirements, please see the Compatibility Matrix on http://www.raritan.com/support . Click Firmware Upgrades and then CommandCenter .
An administrator added a new port to the CC-SG database and assigned it to me, how can I see it in my Ports tree?	To update the tree and see the newly assigned port, click on the Refresh shortcut button on the toolbar. Remember that refreshing CC-SG will close all of your current console sessions.
How will the Windows desktop be supported in the future?	Accessing CC-SG from outside the firewall can be achieved by configuring the right ports on the firewall. The following ports are standard ports: 80: for HTTP access via Web browser 443: for HTTPS access via Web browser 8080: for CC-SG server operations 2400: for Proxy mode connections 5001: for IPR/DKSX/DKX/ P2-SC event notification If there is firewall between two cluster nodes, the following ports should be opened for cluster to be worked properly: 8732: for cluster nodes heartbeat 5432: for cluster nodes DB replication
What are some design guidelines for large-scale systems - any constraints or assumptions?	Raritan provides two models for server scalability: the data-center model and the network model. The data center model uses Paragon to scale to thousands of systems in a single data center. This is the most effective and cost-efficient way to scale a single location. It also supports the network model with IP-Reach and the IP User Station (UST-IP). The network model scales through use of the TCP/IP network and aggregates access through CC-SG, so users don't have to know IP addresses or the topology of access devices. It also provides the convenience of single sign-on.
Authentication	
How many user accounts can be created for CC-SG?	Check your licensing restrictions. There is no specified limit to the number of user accounts that can be created for CC-SG, but the number is not limitless. The size of the database, the performance of the processor, and the amount of memory on the hosting server will determine how many user accounts can actually be created. These user accounts can be any combination of Administrators and Operators with at least one Administrator account.
Can I assign specific port access to a specific user?	Yes, if you have Administrator permissions. Administrators have the ability to assign specific ports per user.

QUESTION	ANSWER
If we had more than 1,000 users, how would this be managed? That is, do you support Active Directory?	CC-SG works with Microsoft Active Directory, Sun iPlanet or Novell eDirectory. If a user account already exists in an authentication server, then CC-SG supports remote authentication using AD/TACACS+ /RADIUS/LDAP authentication.
What options are available for authentication with directory services and security tools such as LDAP, AD, RADIUS, etc.	CC-SG permits local authentication as well remote authentication. Remote authentication servers supported include: AD, TACACS+, RADIUS, and LDAP.
Security	
Sometimes when I try to log on, I receive a message that states my “login is incorrect” even though I am sure I am entering the correct User Name and Password. Why is this?	There is a session-specific ID that is sent out each time you begin to log on to CC-SG. This ID has a time-out feature, so if you do not log on to the unit before the time-out occurs, the session ID becomes invalid. Performing a Shift-Reload refreshes the page from CC-SG. Or, you may close the current browser, open a new browser, and log on again. This provides an additional security feature so that no one can recall information stored in the Web cache to access the unit.
How is a password secure?	Passwords are encrypted using MD5 encryption, which is a one-way hash. This provides additional security to prevent unauthorized users from accessing the password list.
Sometimes I receive a “No longer logged in” message when I click on any menu in CC-SG, after leaving my workstation idle for a period of time. Why?	CC-SG times each user session. If no activity happens for pre-defined period of time, CC-SG logs the user out. The length of the time period is pre-set to 60 minutes, but can be reconfigured. It is recommended that users exit CC-SG when they finish an operation.
As Raritan has Root access to server, this may potentially cause issue with Government bodies. Can customers also have root access or can Raritan provide a method of auditability / accountability?	No party will have root access to server once the unit is shipped out of Raritan, Inc.
Is SSL encryption internal as well as external (not just WAN, but LAN, too)?	Both. The session is encrypted regardless of source, i.e. LAN/WAN.
Does CC-SG support CRL List, that is, LDAP list of invalid certificates?	No.
Does CC-SG support Client Certificate Request?	No.
Accounting	
The event times in the Audit Trail report seem incorrect. Why?	Log event times are logged according to the time settings of the computer that CC-SG is installed on. You can correct this by adjusting the computer’s time and date settings.
Can audit/logging abilities	Direct power switch-off is not logged, but the power on -off

QUESTION	ANSWER
track down to who switched on or off a power plug?	through the CC-SG GUI can be logged to audit logs.
Performance	
As a CC-SG Administrator, I added over 500 ports and assigned all of them to me. Now it takes a long time to log on to CC-SG.	When you, as Administrator, have many ports assigned to you, CC-SG downloads all port information for all ports during the logging process, which slows the process considerably. It is recommended that Administrator accounts used primarily to manage CC-SG configuration/settings do not have many ports assigned to them.
What is the bandwidth usage per client? Particularly as they aggregate up over many systems.	Remote access to a serial console over TCI/IP is about the same level of network activity as a telnet session. However, it is limited to the RS232 bandwidth of the console port itself, plus SSL/TCP/IP overhead. The Raritan Remote Client (RRC) controls remote access to a KVM console. This application provides tunable bandwidth from LAN levels down to something suitable for a remote dial-up user.
Grouping	
Is it possible to put a given server in more than one group?	It should be possible. Just as one user can belong to multiple groups, one device can belong to multiple groups. Edge port groups are simply boolean expressions of attributes. For example, a Sun in NYC could be part of Group Sun: "Ostype = Solaris" and Group New York: "location = NYC"
What impact to other usage that would be blocked through the active usage of the console port, for example, some UNIX variants not allowing admin over network interfaces?	A console is generally considered a secure and reliable access path of last resort. Some UNIX systems allow root login only on the console. For security reasons, other systems might prevent multiple logins, so that if the administrator is logged in on the console, other access is denied. Finally, from the console, the administrator can also disable the network interfaces when/if necessary to block all other access. Normal command activity on the console has no greater impact than the equivalent command run from any other interface. However, since it is not dependent upon the network, a system that is too overloaded to be able to respond to a network login may still support console login. So another benefit of console access is trouble-shooting and diagnosis of system and network problems.
How do you recommend the issue of CIMs being moved / swapped at the physical level with changes to the logical database?	Each CIM includes a serial number and target system name. Our systems assume that a CIM remains connected to its named target when its connection is moved between switches. This movement is automatically reflected in the system configuration and is propagated to CC-SG. If, instead, the CIM is moved to another server, an administrator must rename it.
Interoperability	
How does CC-SG integrate with Blade Chassis products?	CC-SG can support any device with a KVM or serial interface as a transparent pass-through.
To what level is CC-SG able to integrate with 3rd party KVM tools, down to 3rd party KVM port level	3 rd party KVM switches integration is typically done through keyboard macros when the 3 rd party KVM vendors do not publicize the communications protocols for the 3 rd party KVM switches. Depending on the capability of the 3 rd party KVM

QUESTION	ANSWER
or simply box level?	switches, the tightness of integration will vary.
How would I mitigate the restriction of four simultaneous paths through any IP-Reach box, including the roadmap for the potential 8-path box?	Currently, the best possible implementation is to aggregate IP-Reach boxes with CC-SG. In the future, Raritan plans to increase simultaneous access paths per box. These plans have yet to complete development as other projects have taken priority, but we welcome comments about the market demand and use cases of an 8-path solution.
Will the current Paragon boxes work with CC-SG? If not, what is the upgrade path?	The CC-SG V2.0 will work with Paragon that has 3.0 HW and firmware version 3.2 and above. If older versions exist, they must be replaced.
Authorization	
Can authorization be achieved via RADIUS/TACACS/LDAP?	LDAP and TACACS are used for remote authentication only, not authorization.
User Experience	
How will I know if someone else is logged in to leaf nodes?	CC-SG can present the list of users logged in to leaf devices and can show which users are currently accessing an edge port through the active users on a edge port features.
Does CC-SG have the ability to look at multiple screens for devices?	If there are many devices under CC-SG, the user can scroll through the screens to view them all. A user is able to open many screens, each one corresponding to one edge port, but the user is restricted on the KVM side by the actual capacity of KVM over IP channels to be able to access multiple KVM screens.
Regarding console management via network port or local serial port (for example, COM2): What happens to the logging, does CC-SG capture local management or is this lost?	Logging on to CC-SG through the CC-SG console itself is the same as gaining the root privilege of the operating system (Linux) upon with CC-SG is running. Syslog will record such event, but what the user types at the CC-SG console itself will be lost.

North American Headquarters

Raritan

400 Cottontail Lane
Somerset, NJ 08873
U.S.A.
Tel. (732) 764-8886
or (800) 724-8090
Fax (732) 764-8887
Email: sales@raritan.com
Website: Raritan.com

Raritan NC

4901 Waters Edge Dr.
Suite 101
Raleigh, NC 27606
Tel. (919) 277-0642
Email: sales.nc@raritan.com
Website: Raritan.com

Raritan Canada

4 Robert Speck Pkwy, Suite 1500
Mississauga, ON L4Z 1S1 Canada
Tel. (905) 949-3650
Fax (905) 949-3651
Email: sales.canada@raritan.com
Website: Raritan.ca

European Headquarters

Raritan Netherlands

Eglantierbaan 16
2908 LV Capelle aan den IJssel
The Netherlands
Tel. (31) 10-284-4040
Fax (31) 10-284-4049
Email: sales.europe@raritan.com
Website: Raritan.info

Raritan Germany

Lichtstraße 2
D-45127 Essen, Germany
Tel. (49) 201-747-98-0
Fax (49) 201-747-98-50
Email: sales.germany@raritan.com
Website: Raritan.de

Raritan France

120 Rue Jean Jaurés
92300 Levallois-Perret, France
Tel. (33) 14-756-2039
Fax (33) 14-756-2061
Email: sales.france@raritan.com
Website: Raritan.fr

Raritan U.K.

36 Great St. Helen's
London EC3A 6AP, United Kingdom
Tel. (44) 20-7614-7700
Fax (44) 20-7614-7701
Email: sales.uk@raritan.com
Website: Raritan.co.uk

Raritan Italy

Via dei Piatti 4
20123 Milan, Italy
Tel. (39) 02-454-76813
Fax (39) 02-861-749
Email: sales.italy@raritan.com
Website: Raritan.it

Japanese Headquarters

Raritan Japan

4th Floor, Shinkawa NS Building
1-26-2 Shinkawa, Chuo-Ku
Tokyo 104-0033, Japan
Tel. (81) 03-3523-5991
Fax (81) 03-3523-5992
Email: sales@raritan.co.jp
Website: Raritan.co.jp

Raritan Osaka

1-15-8 Nishihonmachi, Nishi-ku
Osaka 550-0005, Japan
Tel. (81) (6) 4391-7752
Fax (81) (6) 4391-7761
Email: sales@raritan.co.jp
Website: Raritan.co.jp

Asia Pacific Headquarters

Raritan Taiwan

5F, 121, Lane 235, Pao-Chiao Road
Hsin Tien City
Taipei Hsien, Taiwan, ROC
Tel. (886) 2 8919-1333
Fax (886) 2 8919-1338
Email: sales.taiwan@raritan.com
Chinese Website: Raritan.com.tw
English Website: Raritan-ap.com

Raritan Shanghai

Rm 17E Cross Region Plaza
No. 899 Lingling Road
Shanghai, China 200030
Tel. (86) 21 5425-2499
Fax (86) 21 5425-3992
Email: sales.china@raritan.com
Website: Raritan.com.cn

Raritan Beijing

Unit 1310, Air China Plaza
No.36 XiaoYun Road
Chaoyang District
Beijing 100027, China
Tel. (86) 10 8447-5706
Fax (86) 10 8447-5700
Email: sales.china@raritan.com
Website: Raritan.com.cn

Raritan Guangzhou

Room 1205/F, Metro Plaza
183 Tian He Bei Road
Guangzhou 510075 China
Tel. (86-20)8755 5581
Fax (86-20)8755 5571
Email: sales.china@raritan.com
Website: Raritan.com.cn

Raritan Korea

#3602, Trade Tower,
World Trade Center
Samsung-dong, Kangnam-gu
Seoul, Korea
Tel. (82) 2 557-8730
Fax (82) 2 557-8733
Email: sales.korea@raritan.com
Website: Raritan.co.kr

Raritan Australia

Level 2, 448 St Kilda Road,
Melbourne, VIC 3004, Australia
Tel. (61) 3 9866-6887
Fax (61) 3 9866-7706
Email: sales.au@raritan.com
Website: Raritan.co.au

Raritan India

210 2nd Floor Orchid Square Sushant Lok 1,
Block B, Gurgaon 122 002 Haryana India
Tel. (91) 124 510 7881
Fax (91) 124 510 7880
Email: sales.india@raritan.com
Website: Raritan.co.in

Raritan OEM Division

Peppercon AG, Raritan OEM Division
Scheringerstrasse 1
08056 Zwickau Germany
Tel. (49) 375-27-13-49-0
Email: info@peppercon.com
Website: www.peppercon.de